2025 BENCHMARKING STUDY

Ethics & Compliance Risk Assessment

Rethink
Compliance

Introduction

Rethink Compliance LLC (Rethink) is committed to driving meaningful change — for our clients, in our industry, and in our clients' workplaces. Every day, we interact with equally dedicated Ethics & Compliance (E&C) practitioners and consistently hear about the value of benchmarking and the crucial role it plays in our industry.

We hope you find this report useful for evaluating and enhancing your own program.

Overview

The utility of an E&C risk assessment is often a debate among E&C practitioners. While some people believe they can be extremely useful, others aren't sure the juice is worth the squeeze.

Despite our individual thoughts and biases on this topic, the reality is that E&C risk assessments are not considered optional by regulators. On the contrary, regulators view E&C risk assessments as foundational requirements for any effective program, and in some industries, regulators view them as mandatory. Our collective goal as E&C practitioners must be to find ways to make the implementation of the assessment process practical, useful, and scalable to our organizations.

We launched our 2025 E&C Risk Assessment Benchmarking Survey to facilitate that very goal, gathering insights directly from E&C practitioners on how they design, execute, and leverage their risk assessments. We are grateful to the over 130 respondents who participated in our survey. Their contributions helped to make this report vital to the E&C field.

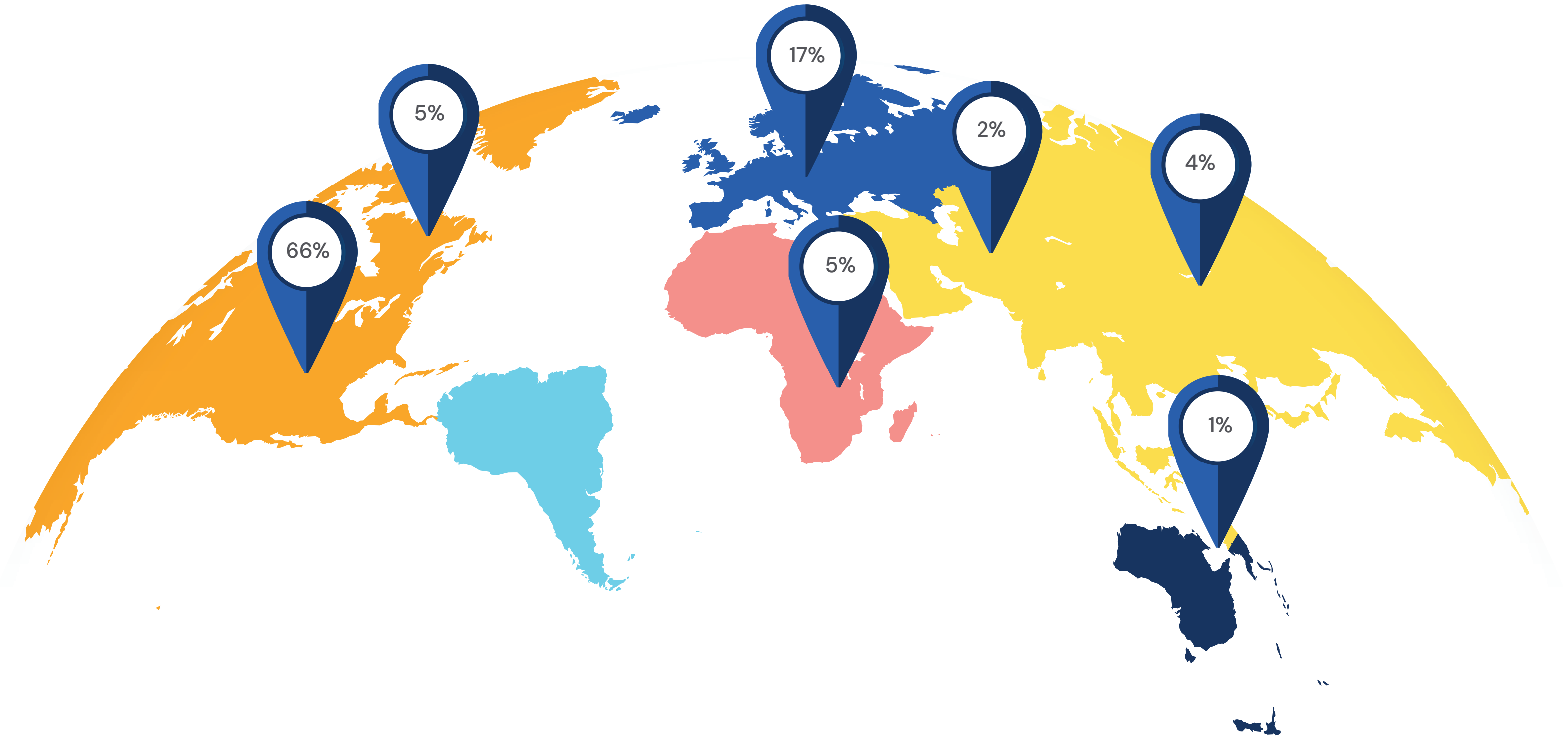
Risk assessment is a new area of benchmarking for Rethink, though our Advisory Services team assists clients in the design and implementation of E&C risk assessments on a regular basis. In our survey, we included questions spanning the development and implementation of E&C risk assessments, on topics ranging from frequency and risk rating methodology to cross-functional involvement and reporting results.

The survey included 33 total questions.

Our respondent pool represents a wide range of organizations across industries, with annual revenue ranging from under $500 million to over $15 billion. They represent both large employers (over 50,000 people) and smaller employers (fewer than 1,000 employees). The majority of respondents work at organizations headquartered in the United States, with some from organizations headquartered elsewhere, including Europe and Africa.

Respondents represented over 20 different industries, including:

- Healthcare Providers
- Life Sciences
- Energy and Utilities
- Technology and Software
- Banking/Financial Services
- Business/Professional Services



HEADQUARTERS — Respondents were global. Almost 30% of responding organizations were headquartered outside of North America.

132 PARTICIPANTS

Ethics and compliance professionals from a wide variety of organizations and industries participated in the survey.

<$500M–$15B+

Our respondent pool represents a wide range of organizations across industries, with annual revenue ranging from under $500 million to over $15 billion.

<1000 employees	>25,000 employees
24%	23%

Small organizations (under 1,000 employees) made up almost a quarter of responses. Larger organizations (over 25,000 employees) represented another quarter of the responses.

A Note on Participation and How to Use This Report

We observed that participation in our E&C risk assessment survey was lower than in our prior benchmarking surveys. On the flip side, we also noted that the percentage of respondents reporting that their organizations engage in both Enterprise Risk Management (ERM) and stand-alone E&C risk assessments was higher than what we have experienced in the field. We hypothesize that these dualities may be explained, at least in part, by a form of selection bias: People at organizations not currently conducting any type of risk assessment may have opted out of participating in this survey, feeling they have nothing to contribute.

Additionally, we noted higher survey participation rates from what we deem to be “more highly regulated” industries (e.g., life sciences, energy/utilities, banking/finance, healthcare). In fact, four of the six industries with the highest number of participants fall into this category. We further hypothesize that a high level of participation by organizations in more highly regulated industries is likely due to the fact that organizations in those industries often have more rigorous E&C programs, due to regulatory requirements.

With that said, this report serves a dual purpose. If you are a reader with an established risk assessment process, you may identify opportunities to enhance maturity and adopt leading practices to improve your risk assessment process. If you are reading this report and have yet to adopt a risk assessment process, you will glean valuable, practical insights from active peers and learn certain strategies to build the internal support necessary to develop an E&C risk assessment process in the future.

Given the different levels of experience our readers may have with risk assessments, we provide some ideas for establishing basic risk assessment protocols in sidebars called “If You’re New to This,” as well as thoughts on maturing an existing program in call outs titled “In Our Experience.”

Our hope is that, by examining how peers are conducting assessments, we will *all* identify opportunities to implement and/or enhance our own E&C programs, no matter where we are in the risk assessment process.

Understanding Risk Assessments

Prior to diving into the study, we thought it would be helpful to provide some background and context around risk assessments in general. A risk assessment is a foundational process for any organization seeking to understand, prioritize, and manage potential threats to its operations and objectives. Organizations use risk assessments to systematically identify what could go wrong, estimate the likelihood and impact of those events, and determine appropriate measures to mitigate them.

While this study focuses primarily on E&C risk assessments, it is important to understand how E&C risk assessments differ from other types of risk assessments, especially enterprise risk assessments (ERAs), as well as how they work together.

ERAs include a broad, strategic review, aiming to capture and prioritize all potential risks — and spanning categories like financial, operational, strategic, and product risks. In contrast, E&C risk assessments have a more focused scope. Their primary purpose is to identify and evaluate specific vulnerabilities related to non-compliance with applicable laws, regulations, and internal policies, as well as the organization's ethical standards and culture.

While ERAs offer a holistic view of potential threats to the entire enterprise, E&C risk assessments drill down to pinpoint vulnerabilities that could lead to misconduct, legal violations (e.g., fraud, corruption, sanctions breaches), and ethical lapses. Though these assessments inform the broader ERA, the E&C risk assessment focus is unique because it allows the organization to thoroughly analyze, and hopefully mitigate, risks tied specifically to legal compliance, integrity, and ethics.

Seventy-eight percent (78%) of our survey participants conduct an ERA. Additionally, 65% conduct a stand-alone E&C risk assessment, indicating that many organizations conduct multiple types of risk assessments across their enterprises.

IF YOU'RE NEW TO THIS

At Rethink, when working with clients, we often use the Three Lines Model (established by the Institute of Internal Auditors) as a framework to help organizations engage all areas of their businesses in risk management. A high-quality E&C risk assessment requires input and action from all three lines:

- **First Line (Management & Operations)**
  Owns and manages risk in day-to-day business. The first line provides crucial input on Inherent Risk (i.e., the levels of risk they face daily).

- **Second Line (Risk, Compliance, & Other Control Functions)**
  Provides expertise, support, and monitoring. The second line designs controls, sets policy, and has a better understanding of Residual Risk (i.e., the levels of risk remaining after controls are applied).

- **Third Line (Internal Audit)**
  Gives independent and objective assurance on the adequacy and effectiveness of risk management and governance across the first and second lines.

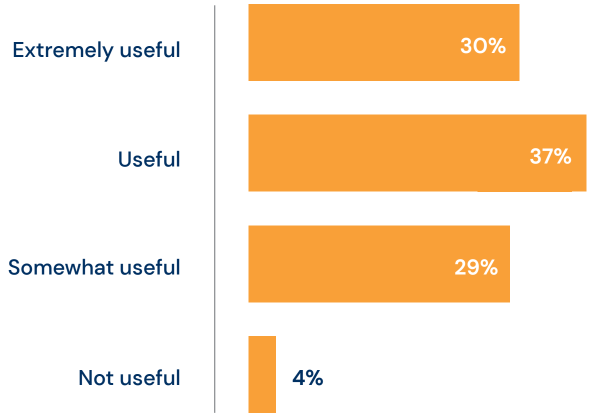
The Three Lines Model is helpful and practical because it clearly defines roles and helps prevent the management of critical risks from falling through the cracks.

Making the Case for Risk Assessments and Why They Are Useful

Interestingly, the vast majority of participants who conduct a stand-alone E&C risk assessment (96%) find them to be useful. Specifically, 30% of those respondents reported their E&C risk assessment is "Extremely useful," 37% find it to be "Useful," and 29% describe their E&C risk assessment as "Somewhat useful."

Only 4% of those participants believe their E&C risk assessment process is "Not useful."

In your opinion, how useful is your E&C Risk Assessment?



IN OUR EXPERIENCE

We were thrilled, but not surprised, to see an overwhelming endorsement of the value of E&C risk assessment from those folks who conduct them. We often hear E&C professionals make statements like "We don't see any value in risk assessments" or "We know our risks." However, our experience working with clients has run counter to this sentiment. When we help organizations implement E&C risk assessment processes, the vast majority report successes similar to the benefits highlighted in our study.

The survey data highlights the following three major areas where respondents find significant value in their E&C risk assessment processes, with only a small minority (2%) reporting no identified benefits.

Raising Awareness and Building Consensus

An E&C risk assessment's value as a communication and alignment tool is evident in survey responses regarding awareness and formalization. The process, when designed appropriately, successfully drives engagement across the organization, starting with leaders: 73% of respondents reported that their E&C risk assessment "has raised awareness of E&C issues with senior management." This awareness also extends to other tiers, with over half of respondents who conduct an E&C risk assessment also reporting increased awareness among middle management.

This broad, cross-functional awareness is directly helpful in breaking down silos. When departments (such as Sales, Legal, and Operations) are brought together to assess a common risk, the process forces necessary conversations, establishes a shared view of threats, and creates a common language for compliance.

This shared view then leads directly to alignment: 47% noted their E&C risk assessment "has led to a documented process and reporting to leadership," and 38% confirmed it "has built management consensus on the top E&C risks." By generating shared data and formal documentation, an E&C risk assessment transforms abstract risks into agreed-upon priorities, facilitating coordinated mitigation efforts across different business units.

Resource Allocation and Risk Identification

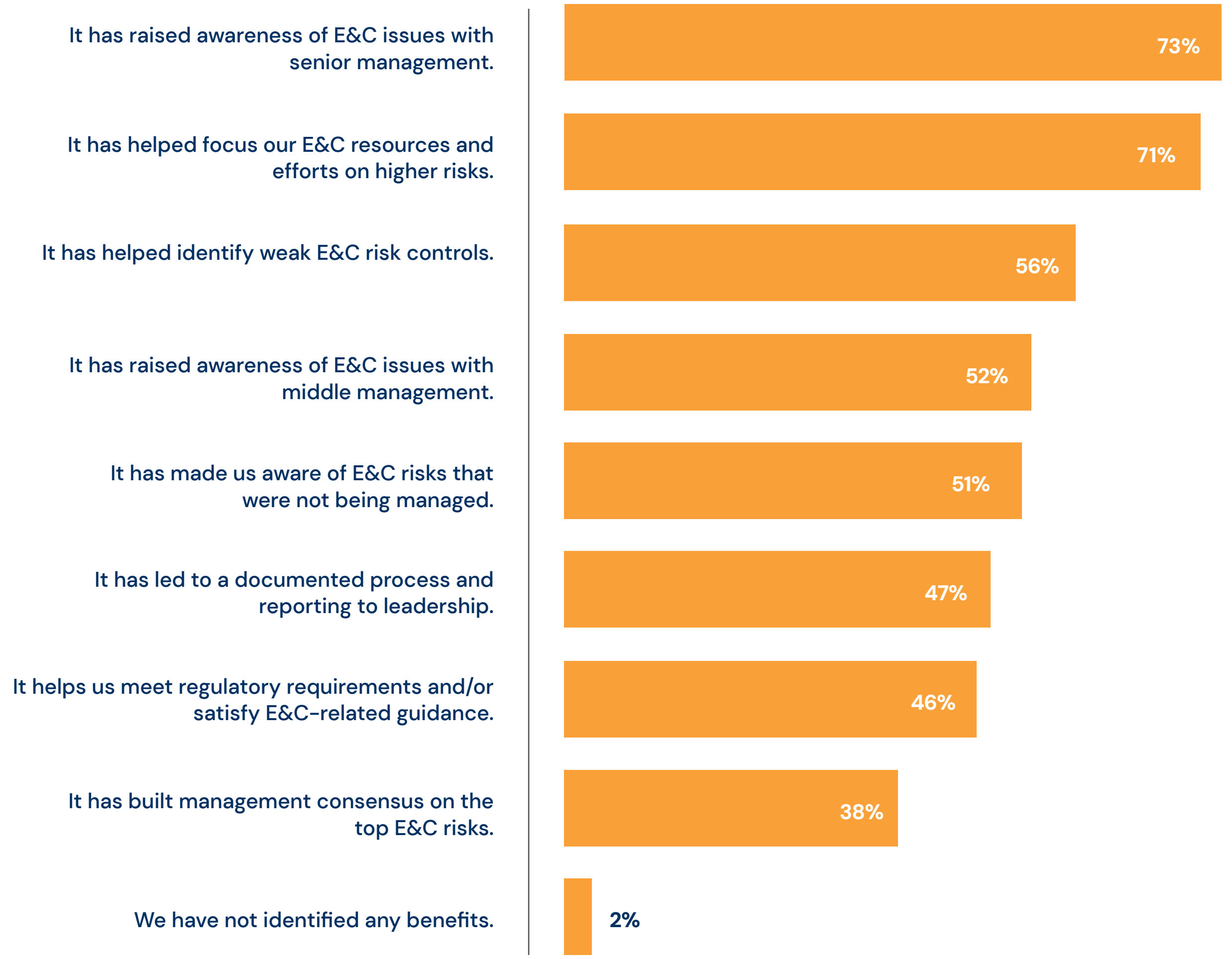
An E&C risk assessment proves its operational value by sharpening the focus of the E&C function and improving understanding of the risk landscape.

- **Optimizing Resources:** Nearly three-quarters (71%) of respondents who conduct an E&C risk assessment reported the assessment "has helped focus our E&C resources and efforts on higher risks."
- **Uncovering Blind Spots:** Respondents also reported that E&C risk assessments can help identify hidden vulnerabilities: 56% indicated it "has helped identify weak E&C risk controls," and over half (51%) stated it "has made us aware of E&C risks that were not being managed."

Satisfying Regulator Requirements or Expectations

E&C risk assessments are a core element of regulatory guidance. (See the U.S. Department of Justice (DOJ)'s Evaluation of Corporate Compliance Programs, September 2024, Sec. I.A (DOJ 2024 Evaluation) and the U.S. Health and Human Services, Office of the Inspector General (OIG), General Compliance Program Guidance, November 2023, Sec. III. F.) They also serve a crucial governance function: Nearly half of respondents who conduct an E&C risk assessment (46%) reported that their assessment "helps us meet regulatory requirements and/or satisfy E&C-related guidance."

What benefits has your E&C Risk Assessment brought to your E&C risk management efforts?



E&C Risk Assessment Processes and Methodologies

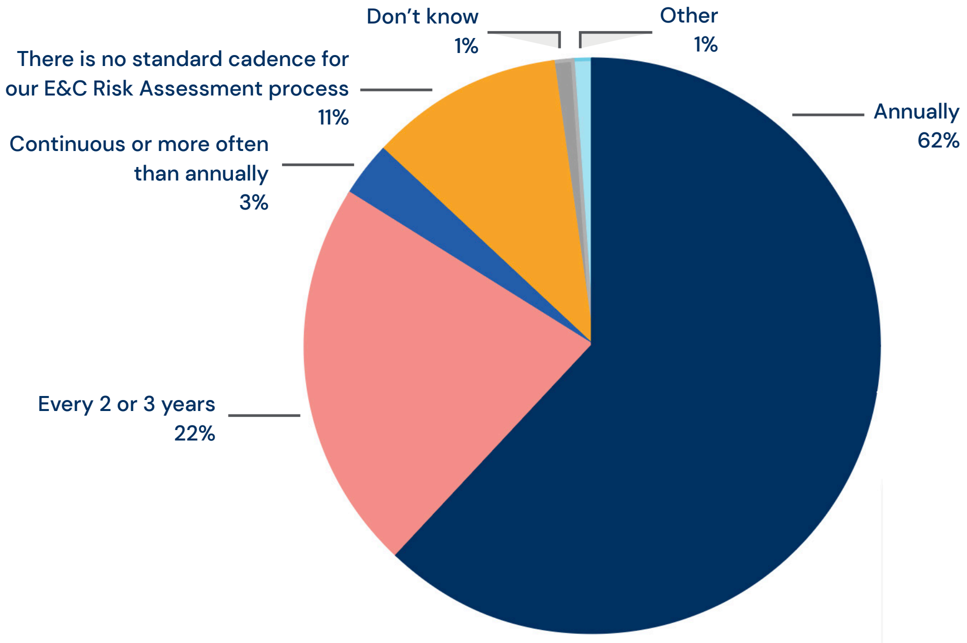
We also examined the methodologies and practices of participants who conduct an E&C risk assessment.

Cadence

The data indicates that an annual E&C risk assessment cadence is the established standard. A clear majority (62%) of respondents who conduct an E&C risk assessment does it annually. Approximately one-fifth (22%) of them use a longer cycle, performing an E&C risk assessment every two or three years. Together, these two primary cadences account for over 83% of responses, indicating that E&C professionals largely prioritize a regular, time-bound review.

A smaller fraction of respondents who conduct an E&C risk assessment (11%) reported no standard cadence for their process, suggesting that, while a fixed cycle is the norm, a few organizations still approach this type of assessment on an ad-hoc or event-driven basis.

How often do you conduct an E&C Risk Assessment?



IN OUR EXPERIENCE

While survey data supports an annual assessment as the standard, our experience at Rethink suggests that the optimal cadence should be evaluated on a case-by-case basis. The frequency of your E&C risk assessment (and other E&C activities) must align with the rate of change in your industry and business model, as well as the expectations of applicable regulators. For example, industries such as Life Sciences and Technology, which face rapidly evolving regulations and business landscapes, respectively, typically deploy an annual or even continuous assessment process. Organizations in other industries with less frequent changes to their footprint, products, or corporate structure may leverage a longer cycle (e.g., every two-to-three years) quite effectively or opt for a phased approach, tackling specific risk areas each year.

IF YOU'RE NEW TO THIS

If you have yet to deploy an E&C risk assessment, don't get too hung up on the cadence. The most important thing is to get started and learn as you go. Document the process and set a cadence after completing one or two E&C risk assessments and determining what works and what doesn't work at your organization.

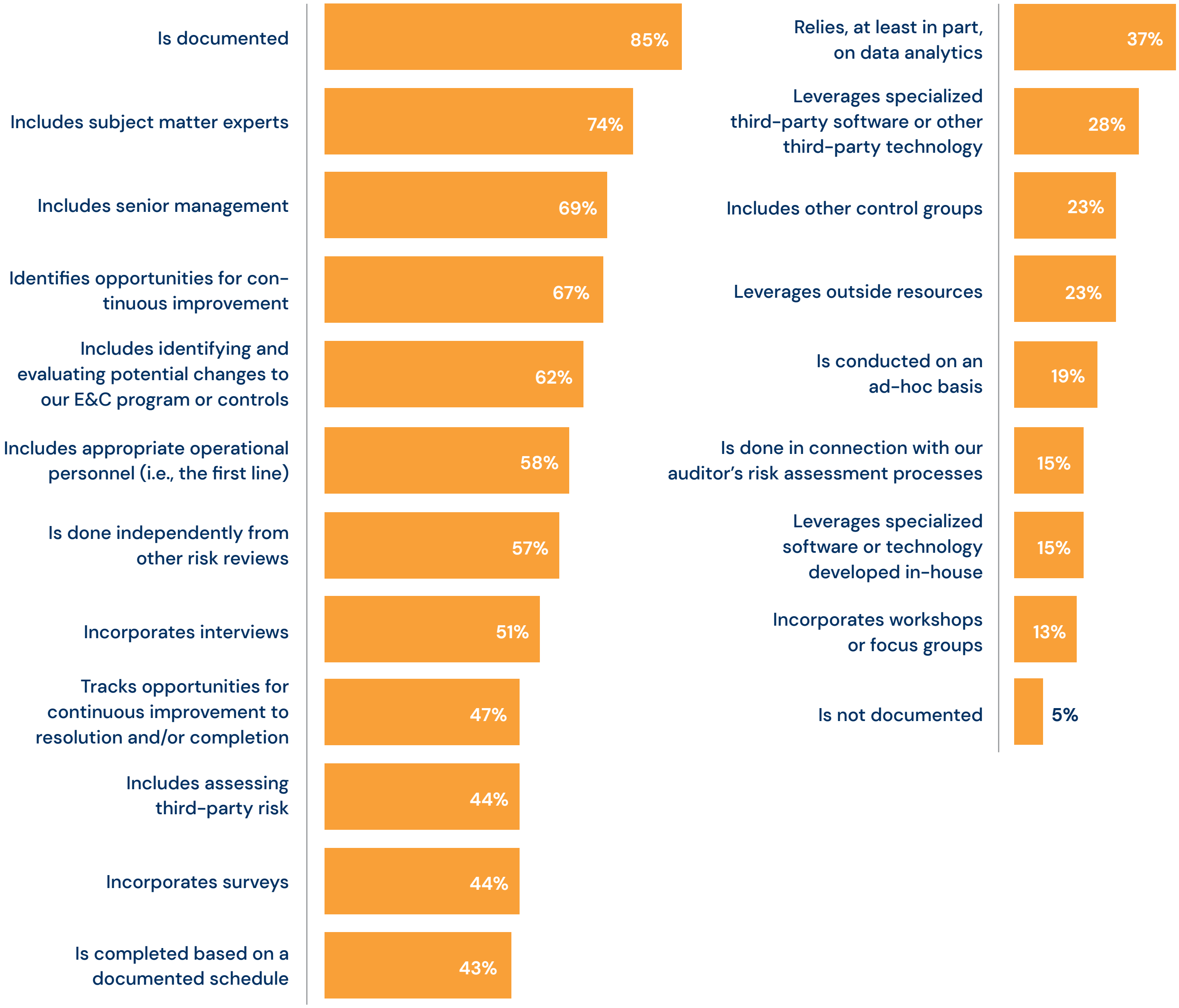
Elements of the E&C Risk Assessment Process

In this section, we provide a look at common E&C risk assessment practices.

A strong consensus exists on the need for structure and broad involvement: The vast majority of respondents who conduct an E&C risk assessment (85%) have documented their process, and significant percentages include subject matter experts (74%) and senior management (69%) in the process. Operational depth is also prioritized, with over half (58%) including appropriate first line, operational personnel. A majority of respondents who conduct E&C risk assessments conduct and incorporate interviews in their processes.

Furthermore, an E&C risk assessment is widely viewed as a tool for change, with 67% of organizations that conduct them using the output to identify opportunities for continuous improvement and to specifically evaluate potential changes to their E&C program or controls.

Our E&C Risk Assessment process:



It is interesting to note that the use of more advanced technological tools and resources is less common. For example, only 37% of participants who conduct E&C risk assessments use data analytics, while only 28% leverage specialized third-party software. As technology continues to evolve and become more accessible, we expect to see an increase in the use of these types of technologies.

IN OUR EXPERIENCE

A robust E&C risk assessment demands structure, broad involvement, and an action plan. For defensibility and effectiveness purposes, we find these priorities are critical:

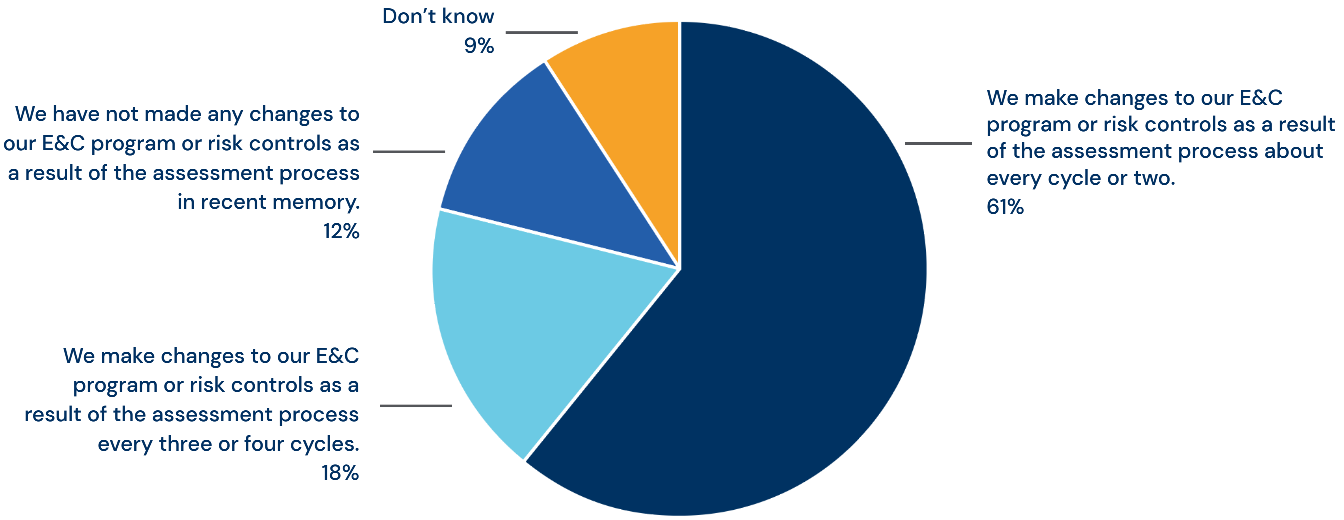
- **Formalize the Process:** The assessment must be documented and scheduled. This is essential as it will indicate to regulators and enforcement agencies that the process is in place and will provide them with information about what is included in the assessment.
- **Involve the Right People:** Systematically include subject matter experts (SMEs), other control groups (i.e., the second line), and especially operational personnel (i.e., the first line), to capture real-world risk.
- **Secure Senior Management Buy-In:** Senior management involvement is vital for raising awareness and securing necessary resources. They are important allies.
- **Look Forward:** Actively consider changes in the legal landscape, new technology, organizational strategy, and changes in operations/your business to stay ahead of emerging risks.
- **Focus on Action and Tracking:** The process must drive continuous improvement. As the DOJ emphasizes, E&C programs must evolve over time (DOJ 2024 Evaluation, Sec. III), and you will need documentation to demonstrate that evolution. Tracking opportunities for improvement through to final implementation is a simple way to demonstrate your program's progression and will serve as a historical reference for internal use. E&C risk assessment output, including suggested improvements, that sits on a shelf with no follow-up is useless.
- **Don't Ignore Third Parties:** For many organizations, one of the greatest risk exposures is external. Make certain your E&C risk assessment includes third-party risks (e.g., trade compliance, bribery, human rights).

Using the Results

As noted above, the DOJ expects E&C programs to evolve over time. Our survey data indicates the vast majority (79%) of organizations do, indeed, take action following an E&C risk assessment.

We also note that action is recurring; the majority of those who implement changes based on the results of their E&C risk assessment (61%) take action every one to two cycles. This finding indicates the assessment is used as a sustained, functional tool to drive regular program adjustments and resource allocation, rather than treated as a one-time formality. This direct link between conducting an E&C risk assessment and implementing subsequent changes confirms its ongoing benefit as a useful tool for maintaining a dynamic, risk-based E&C program.

How often does your organization make changes to its E&C program or its risk controls based on your E&C Risk Assessment results?



IN OUR EXPERIENCE

It is important to be able to show the evolution of your E&C program over time. There are many reasons for implementing changes, such as results of audits, the root cause of incidents or near misses, and the experiences of other organizations. To adequately demonstrate the evolution of your E&C program, you need to document those changes as well.

Considerations When Rating E&C Risks

Ranking residual risk illuminates areas where additional management oversight, controls, or resources may be warranted — and may even identify excessive controls or resources that could be more effectively utilized elsewhere.

We asked participants about the factors they consider in their E&C risk assessments. Survey results confirm that E&C practitioners are prioritizing the fundamental factors of risk, with 87% considering risk **impact** and 86% considering risk **likelihood** in their E&C risk assessment design. In addition, over 78% consider **inherent risk,** and 63% consider **residual risk.**

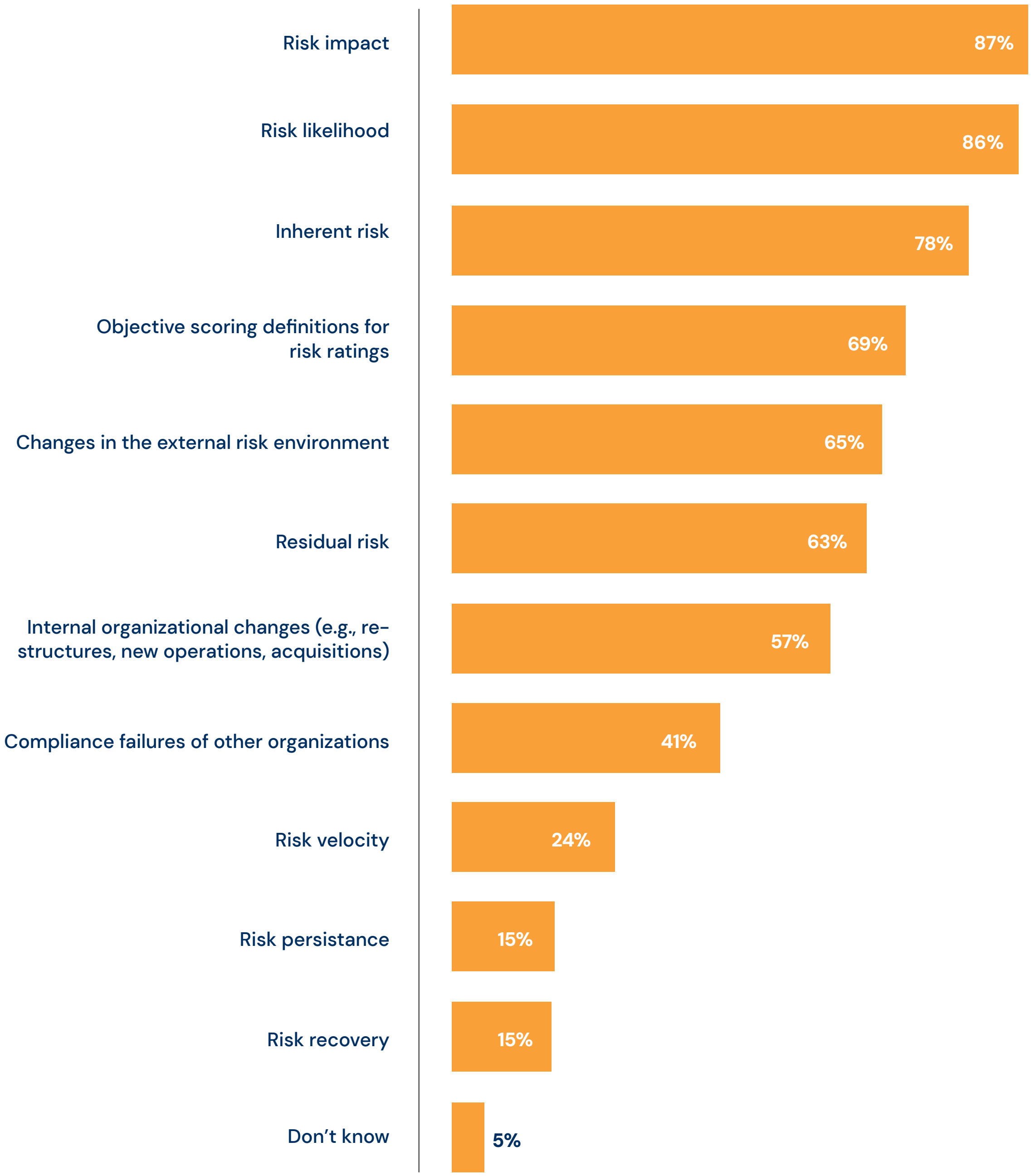
The data also reveals that most organizations have moved toward formalizing the rating process, with 69% noting that they use objective scoring definitions for risk ratings. Objective definitions are essential for achieving meaningful comparisons and consensus. Furthermore, organizations recognize the need for a dynamic process that accounts for change, with 65% noting that they consider changes in the external risk environment and 57% indicating they look at internal organizational changes (e.g., restructures, acquisitions).

IF YOU'RE NEW TO THIS

When assessing risk of any kind, consider the two most important factors: the **impact** of the risk if it were to occur and the **likelihood** of the risk occurring. When rating a risk, organizations usually use a formula to combine the likelihood and impact for a final risk rating. Building on this foundation, a leading practice in risk management is to identify both **inherent risk** (the impact and likelihood of the risk before controls are considered) and **residual risk** (the impact and likelihood of the risk after existing controls are factored in).

In contrast, lower percentages of respondents considered more advanced or nuanced factors, such as **risk velocity** (24%), **risk persistence** (15%), and **risk recovery** (also 15%). Depending on your industry and the types of E&C risks you encounter, these elements may be valuable for fine-tuning risk rating and control design.

In designing your E&C Risk Assessment, which of the following does your organization consider?



E&C Risk Catalog

E&C risk assessments vary significantly from organization to organization, reflecting the unique nature of every business. A **"risk catalog"** or **"risk register"** is the list of potential risks an organization deems relevant to its operations and is useful in the management of those risks. This register (or catalog) should not only list the threats the organization faces, but also include key context, such as the functions where those risks are likely to emanate and the specific types of risks or threats. In this way, risk catalogs can help the E&C team determine risk-related responsibilities across the business to identify risks that may be orphaned.

Our survey data indicates that the majority of respondents prioritize a fairly detailed classification and risk ownership when designing their E&C risk catalog.

The most commonly included information focuses on categorization:

- A strong majority (85%) include the high-level category of E&C risk (e.g., bribery, competition law).
- Three-quarters of organizations go a step further to include subcategories of E&C risk (e.g., breaking down "competition law" into "price fixing" or "bid-rigging"), which allows for a more granular and actionable analysis.

Organizations also widely incorporate the dimensions of risk ownership and control groups.

- 61% include first-line risk ownership (i.e., the departments or groups whose activities create the risk).
- 53% identify the second-line function responsible for giving expert advice, designing controls, and providing other assistance.
- Approximately half consider geographical E&C risk.

IN OUR EXPERIENCE

An E&C risk assessment's value is in its ability to drive meaningful comparisons among various risks and suggest appropriate program adjustments. At Rethink, we have found that establishing the basics is imperative.

Find a way to consistently describe your risks:

- **Written Definitions:** Develop written definitions for risk ratings that include objective landmarks (e.g., specific penalty sizes, potential monetary losses, effect on operations, and type of reputational damage).
- **Risk Tolerance/Appetite:** The risk rating definitions effectively set an organization's risk appetite. These definitions should be approved by senior management and possibly even the Board.

Stay On Top of Emerging Risks:

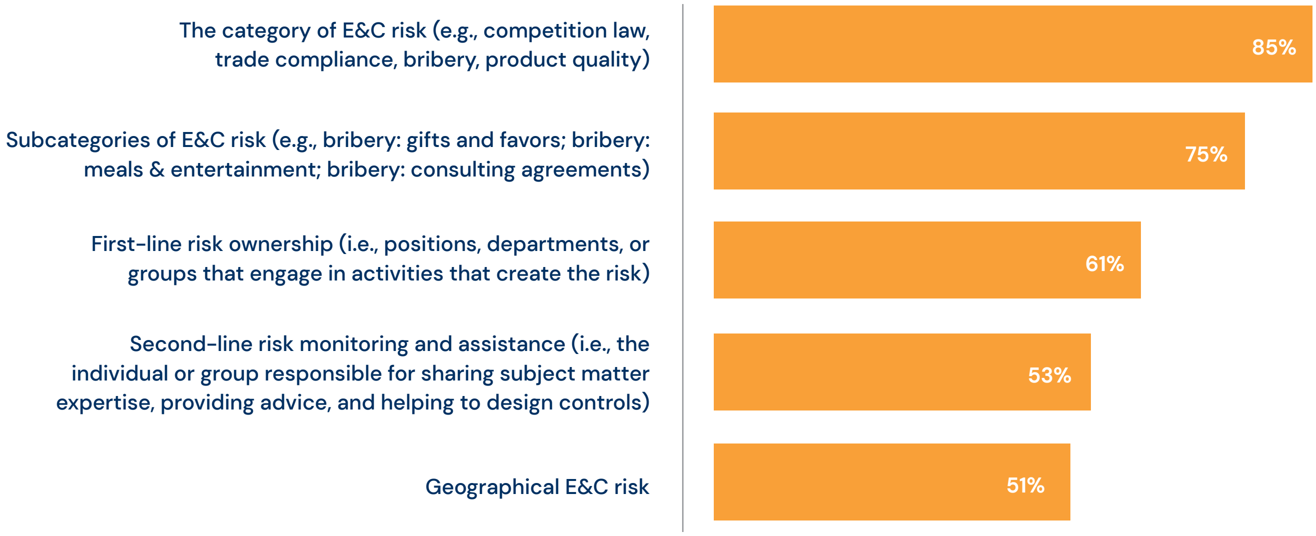
A stagnant assessment is useless. It must include a dynamic process and outputs that reflect your current operating reality.

- **Integrate Change:** Assess the impact of recent and planned operational, organizational, and business changes (e.g., acquisitions, new products, new locations).
- **Look Externally:** Account for the external landscape by including shifts in laws, enforcement trends, and compliance failures by other organizations. It is always better to learn from others' mistakes.

IF YOU'RE NEW TO THIS

Start Simple: While quantitative definitions are the goal, starting with a basic qualitative scale (like Red, Yellow, Green) can be a way to simplify the process for those participants who are new to the concept.

What information is included in your E&C risk universe, E&C risk catalog, or list of risks compiled during your E&C Risk Assessment process?

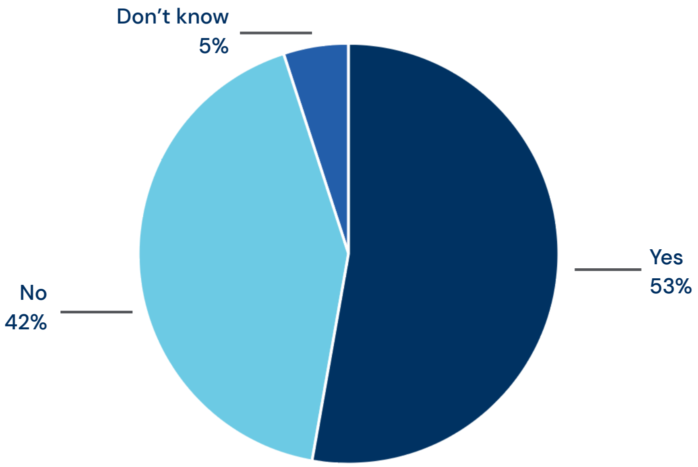


What type of dimensions to include will vary by organization. The DOJ cites factors such as location, potential clients and business partners, and payments to officials or governments. For small organizations with limited operations, it may not be insightful to keep track of geographical risks. For multi-national organizations, where risks increase or decrease based on geography, this element is helpful to include.

Use of KPIs/KRIs:

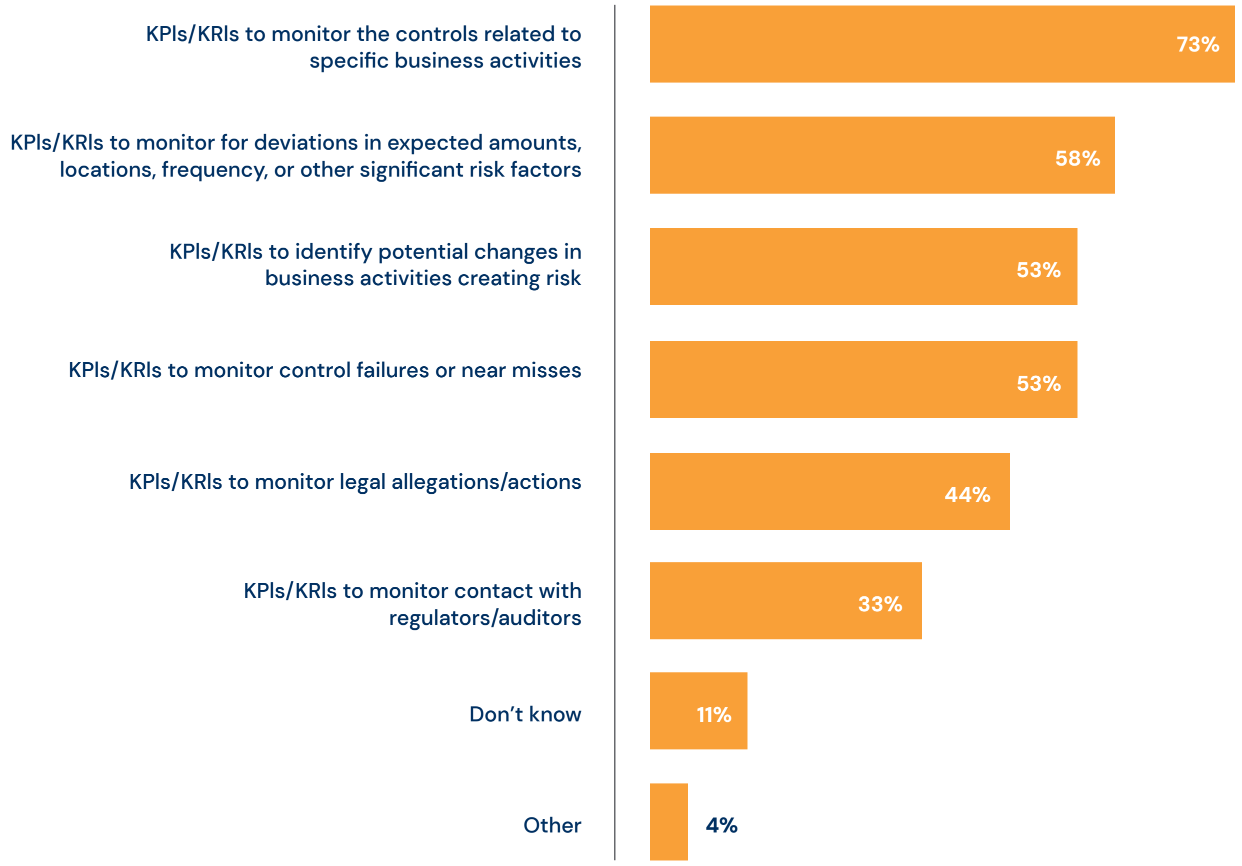
The use of key performance indicators (KPIs) and key risk indicators (KRIs) as part of a risk management process is becoming a key practice, with 53% organizations that conduct E&C risk assessments reporting their use. This reliance on metrics aligns directly with the DOJ's emphasis on using data and systems to continuously improve an E&C program.

Do you use key performance indicators (KPIs) or key risk indicators (KRIs) in your organization's management of E&C risks?



Specifically, at the 53% that use KPIs or KRIs, they are most commonly used to monitor controls related to specific business activities (73%). Over half of these organizations also use them to monitor deviations in expected amounts, locations, or frequency, or other significant risk factors (58%) and to identify potential changes in business activities creating risk (53%). A significant percentage (53%) use these metrics to track control failures or near misses, providing proactive insight into where the E&C program may be in need of improvement before a major violation occurs.

What type of KPIs or KRIs does your organization use in its E&C risk management program?



IN OUR EXPERIENCE

The DOJ and other regulators and enforcement agencies expect organizations to actively use data to identify potential misconduct and to flag deficiencies in their E&C programs. Beyond simply meeting these expectations, leveraging data provides valuable, high-volume insights that would be impractical to gather manually.

Consider these examples for using data in compliance monitoring:

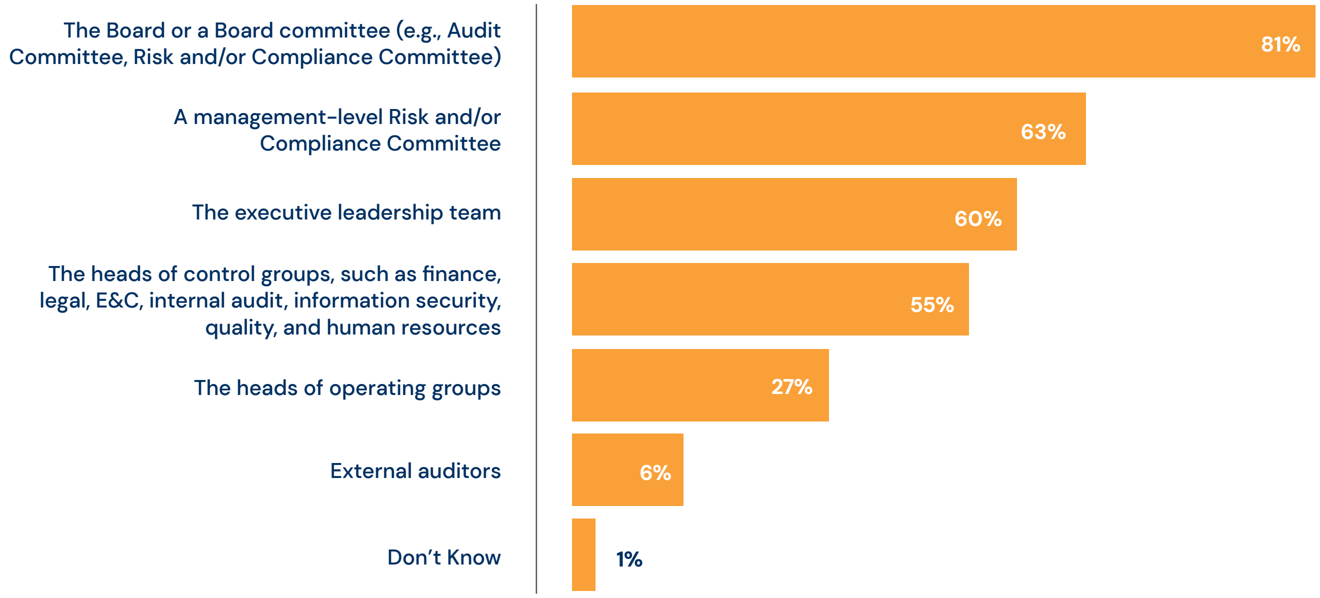
- **Monitor Control Process Patterns:** Use data from existing control processes to track deviations from normal patterns. A change — such as a sharp drop in books-and-records entries — could signal a contracting business unit, or it could reveal that employees are bypassing a control, indicating a need for better training or a simpler process.
- **Track Engagement and Guidance Needs:** Track usage of the Code of Conduct, helpline inquiries, and policy views for shifts in volume or topical interest. Analyzing the root cause of these changes — whether an increase or a decrease — can highlight the need for targeted guidance, changes in operations, or focused training for new employees or managers.

Reporting Results

A substantial majority of respondents (81%) note that they report E&C risk assessment findings to the Board of Directors or a Board committee (e.g., an audit, risk, or compliance committee). Nearly two-thirds of organizations (63%) report E&C risk assessment results to a management-level risk and/or compliance committee, and 60% of respondents report assessment results to the executive leadership team.

Over half of organizations share assessment results with heads of control groups (e.g., legal, internal audit, human resources), helping facilitate cross-functional alignment. However, reporting to the heads of operating groups is notably less frequent (27%).

To whom do you report the results of your E&C Risk Assessment?



The percentage of organizations reporting to the Board and management is encouraging. Opportunities to report are critical for gaining management support for the E&C program as well as for building cross-functional awareness of important issues. The use of management-level risk and compliance committees has been growing as the E&C profession has matured. Risk and compliance committees are specifically mentioned by the OIG and can serve as powerful allies to help improve controls and your overall E&C program.

IN OUR EXPERIENCE

At Rethink, we believe that a high-impact E&C risk assessment requires broad engagement throughout the process, not just at the final sign-off. Working across the organization will ultimately help make your risk assessment process much more successful. Depending on their role, different stakeholders can be involved at different levels, with some playing an active role and others simply receiving the final report.

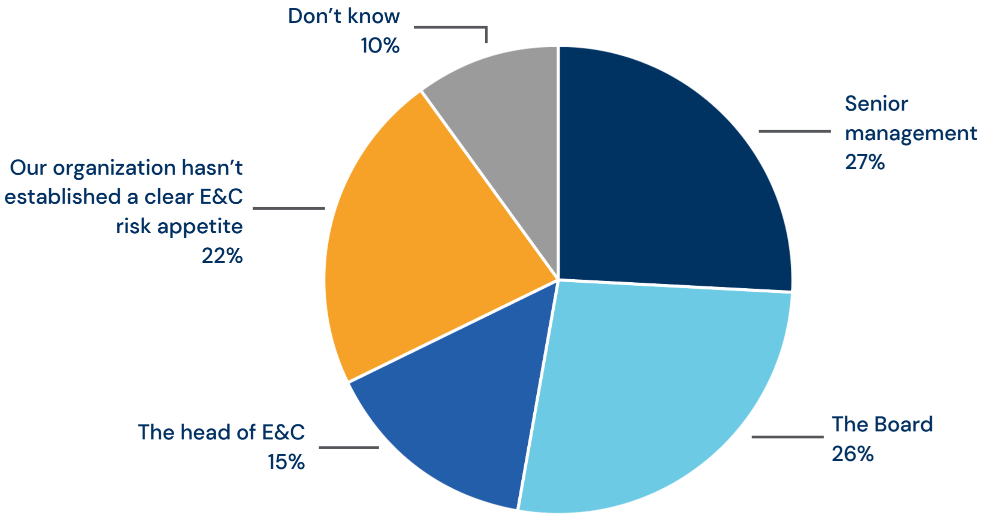
- **Management-Level Risk or Compliance Committee:** Involving your management-level risk or compliance committee in your entire E&C risk assessment process is very helpful. Involvement will depend on the committee's charter and scope of responsibilities, and if leveraged effectively, the committee will serve as a key player in identifying and implementing improvements.
- **Operating Groups:** Operating groups are essential because they have the most familiarity with the day-to-day business activities that create risk. Their input is critical for accurately identifying and assessing inherent risk and gauging the effectiveness of current controls in determining residual risk. Their insight and cooperation are critical for improving controls.
- **Operating Heads:** Making these leaders aware of the E&C risks their teams face enables them to directly manage those risks more effectively.
- **Auditors:** Internal audit is routinely involved in both the E&C risk assessment process and follow-up. In contrast, external auditors are typically only involved when the organization specifically requires independent external review.

Risk Appetite

For an E&C program to be effectively managed, it must be guided by a defined risk appetite or risk tolerance — in other words, how much risk the organization is willing to handle. Our survey results suggest that risk appetite/tolerance is most often set by senior management or the Board, with the Board being leading practice, especially at large, public companies.

Notably, 22% of respondents reported that their organization has not set a risk appetite. By using consistent risk rating definitions, management can communicate what level of risk it is willing to accept overall or in specific areas. For example, the Board may say the organization should not have any E&C risks above a specified level. Establishing a defined risk appetite is essential for properly prioritizing efforts, justifying a program's resource allocation, and determining which controls to implement, especially if ever scrutinized by regulators or enforcement agencies such as the DOJ.

Who sets the E&C risk appetite for your organization?



IN OUR EXPERIENCE

Setting risk appetite requires identifying key elements of concern, such as monetary loss, legal costs, operational interruptions, and reputation — and then clearly defining the acceptable levels of potential consequences for each. Since some organizations tolerate more severe consequences, setting a higher acceptance level in these areas ultimately means that fewer, or less robust, controls are needed to bring the residual risk down to an acceptable level.

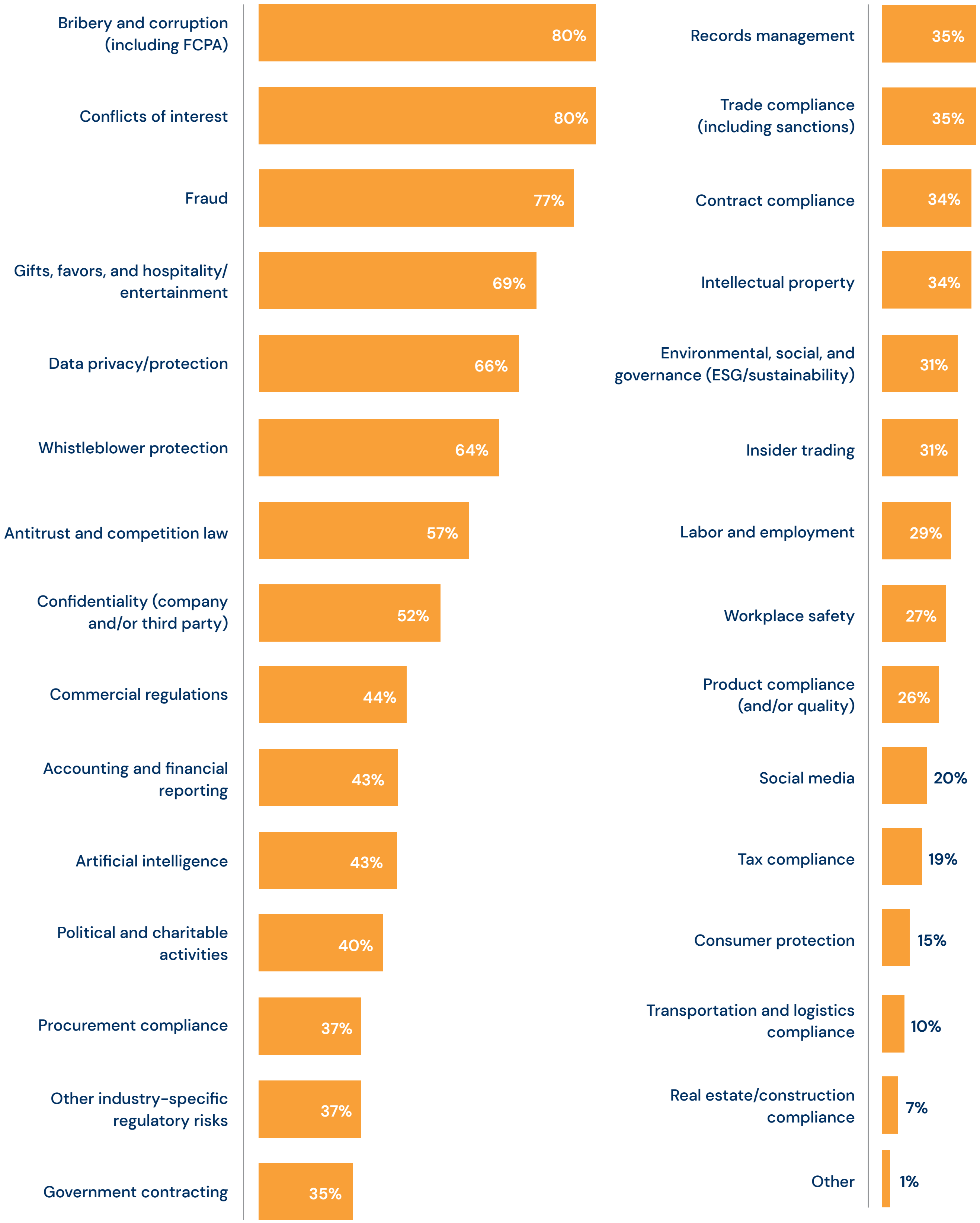
Risks Assessed

The risk areas included in an E&C risk assessment are usually driven by the scope of responsibilities of the E&C function. Most respondents clearly prioritized core integrity risks (e.g., bribery and corruption, conflicts of interest), but there was significant variation in the coverage of other areas, which makes sense given that every organization has a unique structure and risk profile.

We are concerned, however, about coverage gaps in newer risk areas. Consensus sharply drops for emerging risks such as artificial intelligence; rapidly evolving risks, including trade compliance; and frequently orphaned risks like environmental, social, and governance/sustainability. The variations in response set forth in the chart on the next page indicates that, while most fundamental E&C risks are typically covered, organizations are well advised to more adequately address the evolving risk landscape for all E&C-related risks.

This pattern suggests E&C risk assessments are highly successful in covering traditional financial crimes and behavioral ethics risks, but many are still maturing in their approach to regulatory, operational, and technology-driven compliance challenges.

Which of the following risks do you assess in your E&C Risk Assessment?



IN OUR EXPERIENCE

One of the most important things for E&C professionals to understand and remember is that we don't have to own each risk — in fact, we should own very, very few — but we need to know who does. Our primary goal should be developing clarity about which internal group is responsible for managing and monitoring significant E&C risks (e.g., who is controlling third-party risks, product risks, social media risks, etc.). A major benefit of this clarity is preventing "orphaned" E&C risks — those that no one is sufficiently managing or monitoring — which we frequently uncover when helping clients build their E&C risk assessment and risk management programs.

Controlling risks requires open collaboration with specialized SMEs from the first and/or second lines. At Rethink, we often see strong working relationships develop between information technology (IT) security and E&C, for example. Often IT security assesses its own risks and implements controls, but partners with E&C or legal to handle data security requirements and data privacy laws.

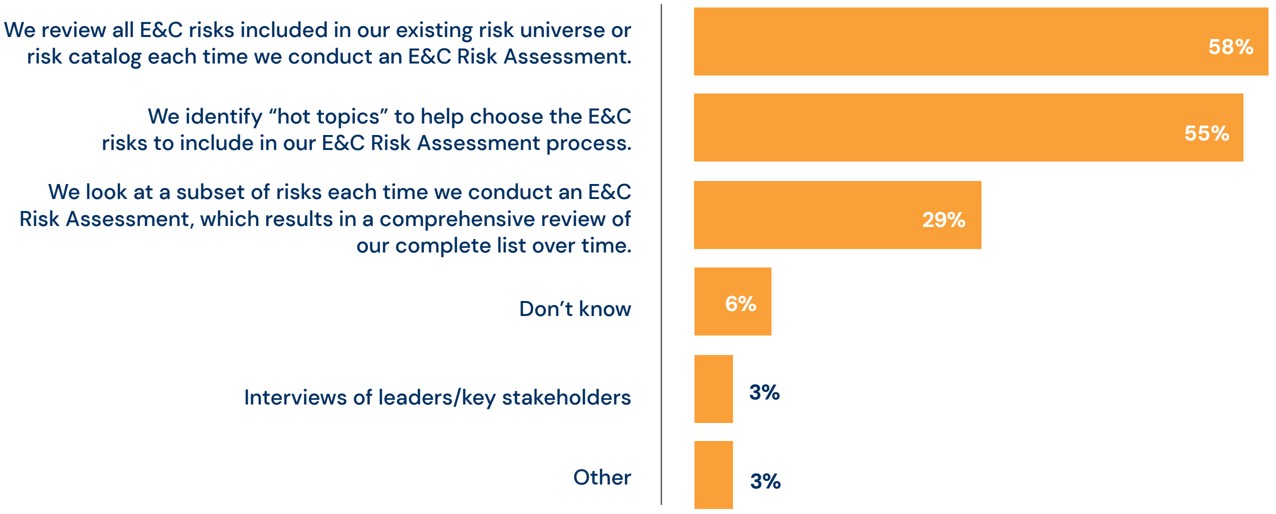
It's important for all of us to remember that there is no need for the E&C group to get into the weeds of highly specialized risks if those risks are already being assessed and monitored effectively by established experts. We just need to kick the tires to satisfy ourselves that they have an effective process.

Cadence of Risk Reviews

When deciding how often to refresh their E&C risk assessments, respondents use different strategies, balancing a structured review against the need to address current issues. Our survey data reveals that 87% of respondents are committed to comprehensive risk review. They cover all known E&C risks either annually or on a rotational basis over time. We recommend this practice, as it prevents organizations from ignoring a risk that may grow from insignificant to a major concern over time.

The data also suggests that over half of those responding incorporate an examination of "hot topics" when selecting what E&C risks to assess in their process. While addressing these timely issues is important, this approach should be used in connection with a structured review of all known risks.

How do you determine which risks to include in your E&C Risk Assessment?



Integrating Assessment Results Into Training

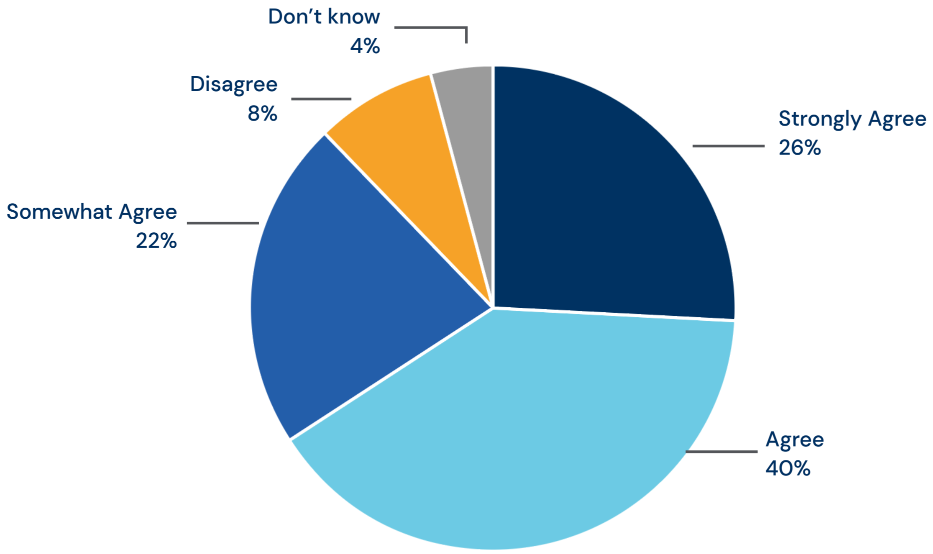
When working with clients to develop and deploy E&C risk assessments, we often see that the risk assessment exercise is not just a theoretical exercise; it is actively used to design programs, allocate resources, and prioritize training.

The data supported that a large majority of respondents who conduct E&C risk assessments use their risk assessment as a foundational tool. Specifically, 86% of those respondents reported that their E&C training program is shaped by their assessment results. This high percentage indicates that the assessment isn't just a report; it's a functioning part of the E&C program that leads to a training program focusing on the most important risks, rather than simply addressing the loudest voices or the "squeaky wheel."

IF YOU'RE NEW TO THIS

For organizations just establishing their E&C risk assessment, focusing on current hot topics is an excellent, practical way to gain initial leadership attention and build a platform to mature the comprehensive risk assessment process over the next few years.

Our E&C training program is informed by our E&C Risk Assessment results.



Program Design and Resources

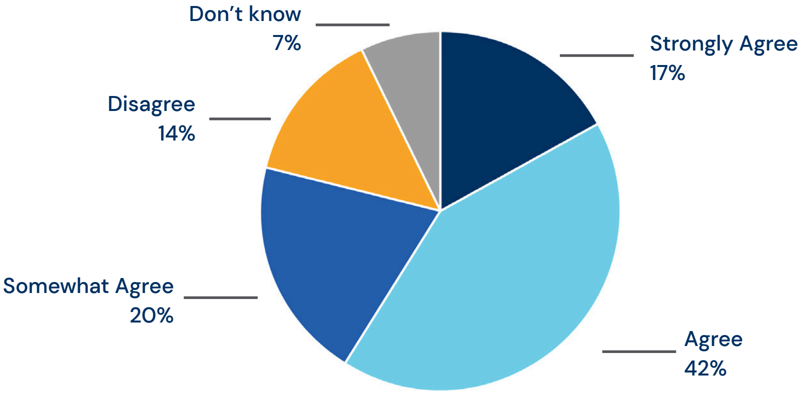
The primary goals of an E&C risk assessment are to help organizations design their E&C program effectively and control their risks well with the resources they have. Our survey results, however, reveal a key tension between perceived design and practical execution.

A significant majority of all survey participants (79%) generally believe their programs are appropriately designed to address their E&C risks, and 84% at least somewhat agreed there is a strong correlation between their highest E&C risks and the controls and resources dedicated to managing them, which is a key component of an effective program design.

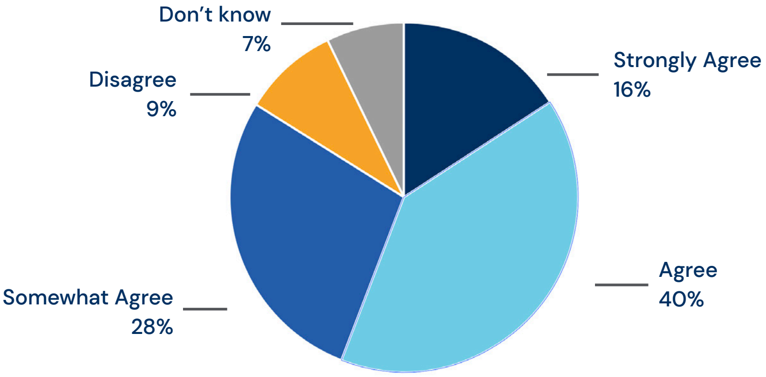
While overall those numbers are encouraging, a closer look suggests there is still work to be done.

- Only 62% of total respondents agreed or strongly agreed that their programs are resourced commensurate with their organization's E&C risks.
- Only 56% of total respondents agreed or strongly agreed that there is a strong correlation between their highest risks and the resources dedicated to managing those risks.

The design of the E&C program at our organization and our available E&C resources are commensurate with the organization's E&C risks.



At our organization, there is a strong correlation between the highest E&C risks and the controls and resources dedicated to managing those risks.



Said another way, over half of total respondents are not confident that (i) their resources are commensurate with organizational risks or (ii) their highest risks are appropriately covered.

E&C risk assessment execution can, and should, vary among organizations. However, a well-designed program is the ultimate goal, and the data suggests that about half of our respondents have significant reservations about meeting that standard. Some of the open-ended comments provided at the end of our survey indicate E&C groups feel under-supported by management or have limited ability to build and improve their programs based on limitations set by higher management.

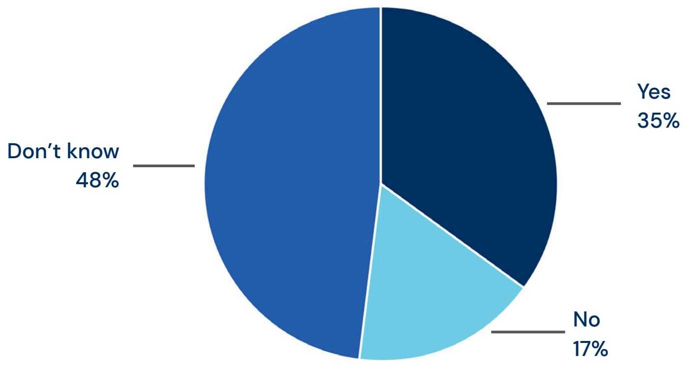
We anticipate confidence in the design of organizations' E&C programs will increase as E&C functions continue to mature and are, hopefully, increasingly viewed by the business as a strategic partner that helps achieve goals, rather than simply as a gatekeeper.

E&C Risk Assessment Adoption: Plans and Priorities

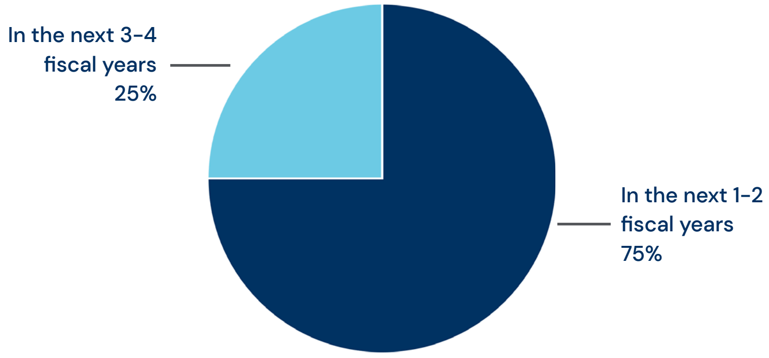
Of the 46 organizations that are not currently conducting an E&C risk assessment, 35% expressed that they plan to conduct one in the future, with only 17% stating that they do not have any plans to do so. It is noteworthy that, of those who do plan to conduct an E&C risk assessment, 75% report they will do so in the next one to two fiscal years and 25% plan to within the next four fiscal years. It's a positive sign that the use of E&C risk assessments continues to grow among organizations.

The primary reasons this audience does not conduct an E&C risk assessment include that they assess E&C risks as part of a larger organizational process (38%), lack resources, or are at a small organization. Again, each organization has to manage its own program based on its needs, budget, and other important business factors.

Do you plan to conduct a formal E&C Risk Assessment in the future?



What is your timeline to start an E&C Risk Assessment?



Conclusion

Thank you for your interest in this report. We trust the data and insights we have shared will help you benchmark your program and advance your strategic thinking on how you approach E&C risk assessments.

As you consider the insights shared, remember that a risk assessment is not merely a program design tool. It is a critical exercise that helps build awareness, create internal consensus, and proactively identify potential risks across the enterprise.

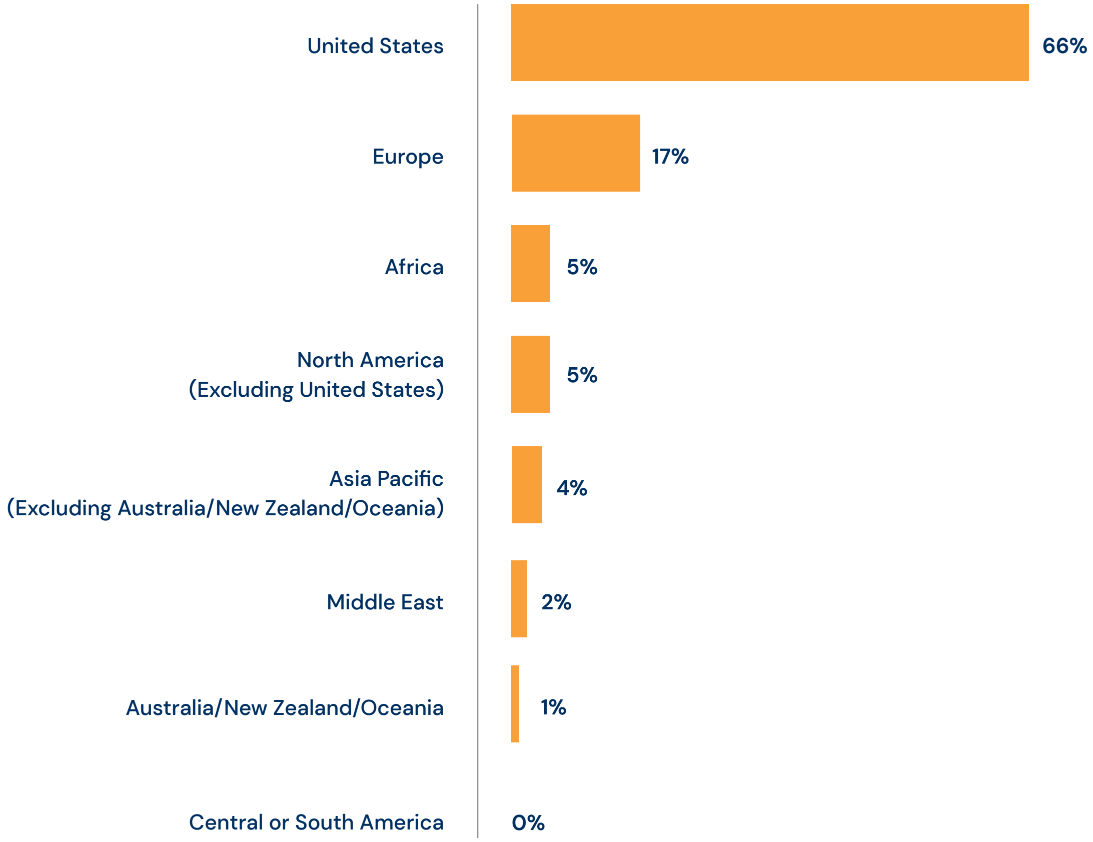
We also trust this report will be helpful regardless of where you are in the process. For those of you already conducting an E&C risk assessment, we've aimed to provide actionable ideas for improvement. For those of you still exploring how to implement an E&C risk assessment, we hope we have offered guidance and support as you begin your journey.

Our benchmarking efforts would not be possible without your contribution. We will look forward to your participation in future Rethink surveys. We also hope that, the next time we conduct a survey on this element of an effective E&C program, we will find that even more organizations have formal E&C risk assessments in place and are ready to add their insights to our collective benchmarking.

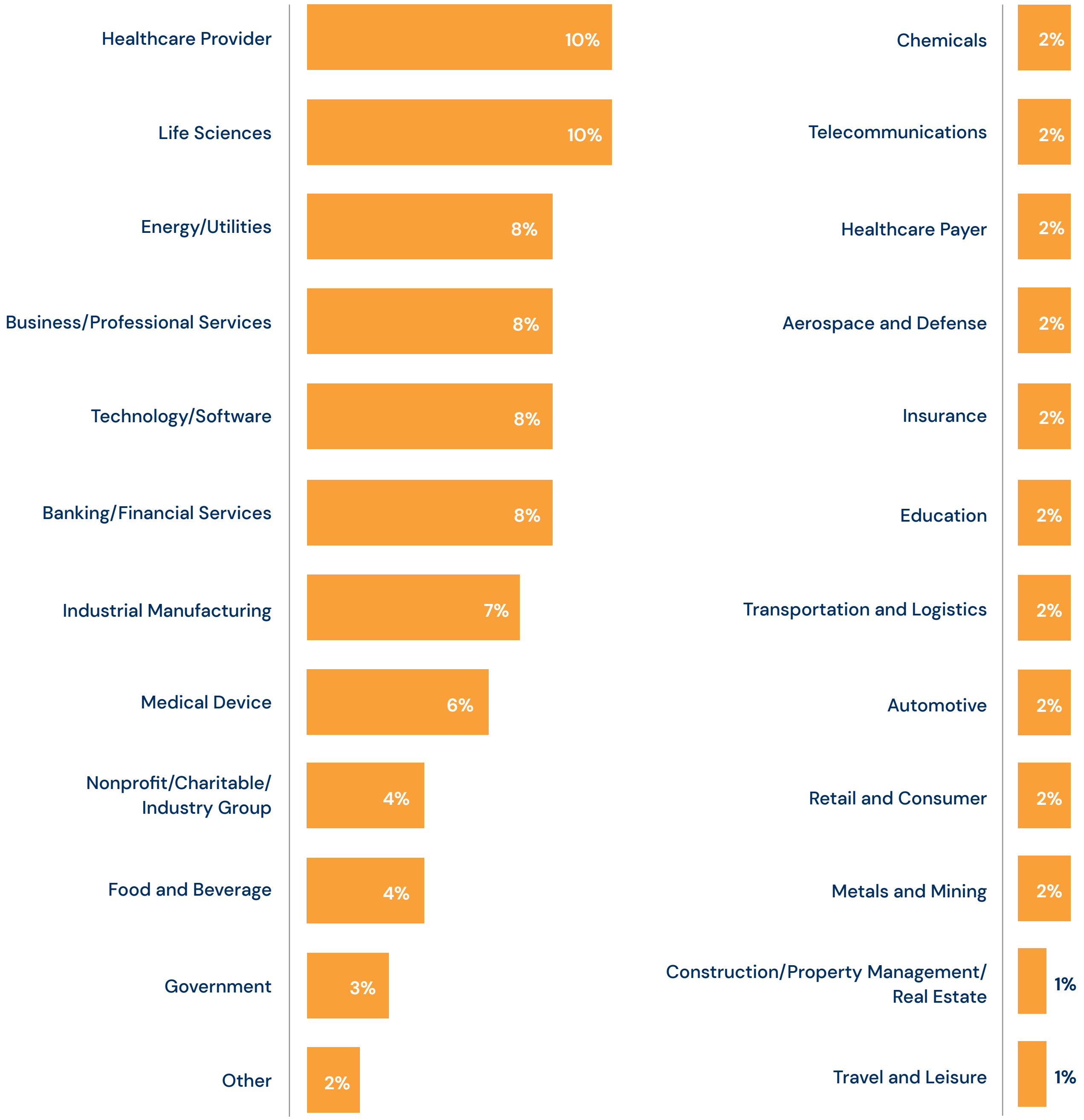
We encourage you to continue shaping industry-leading practices by participating in our future benchmarking surveys. Remember: benchmarking is only possible if we *all* contribute our time and energy in pursuit of the ultimate goal.

Appendix

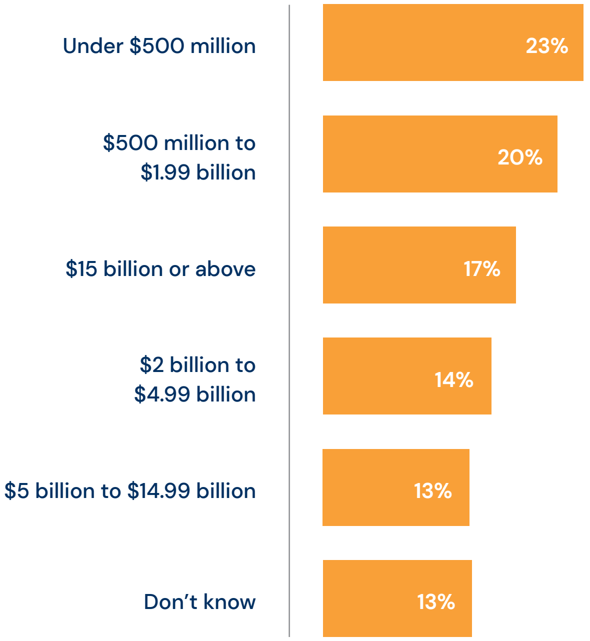
In what region is your organization headquartered?



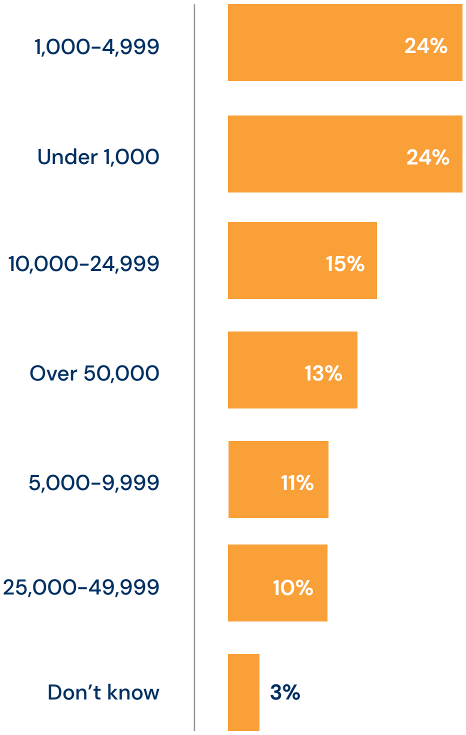
Which of the following most closely describes your organization’s industry?



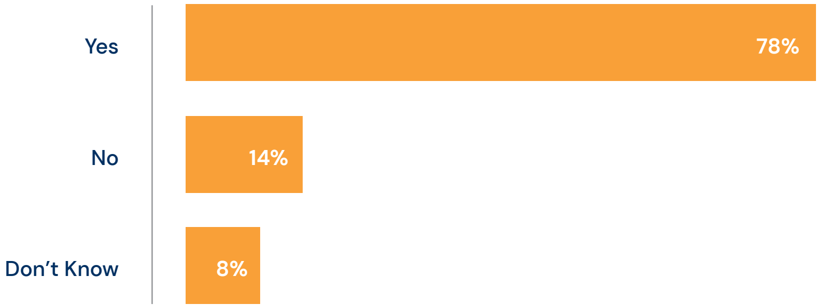
What is the approximate annual revenue of your organization in U.S. dollars?



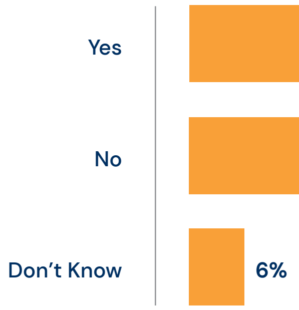
How many employees work in your organization, globally?



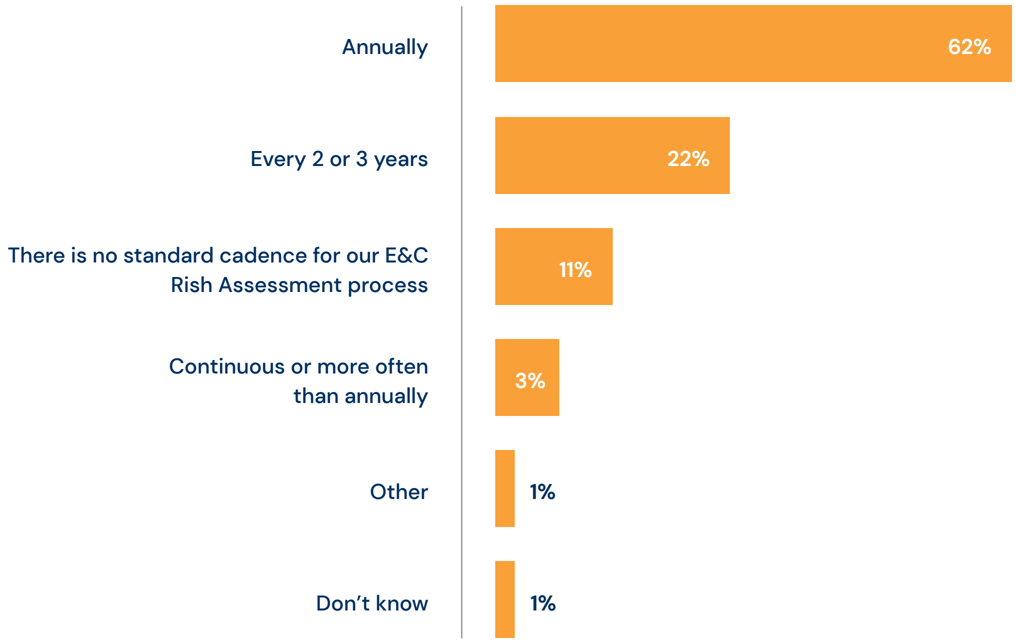
Is there an enterprise risk assessment (ERA) process or an enterprise risk management (ERM) program at your organization?



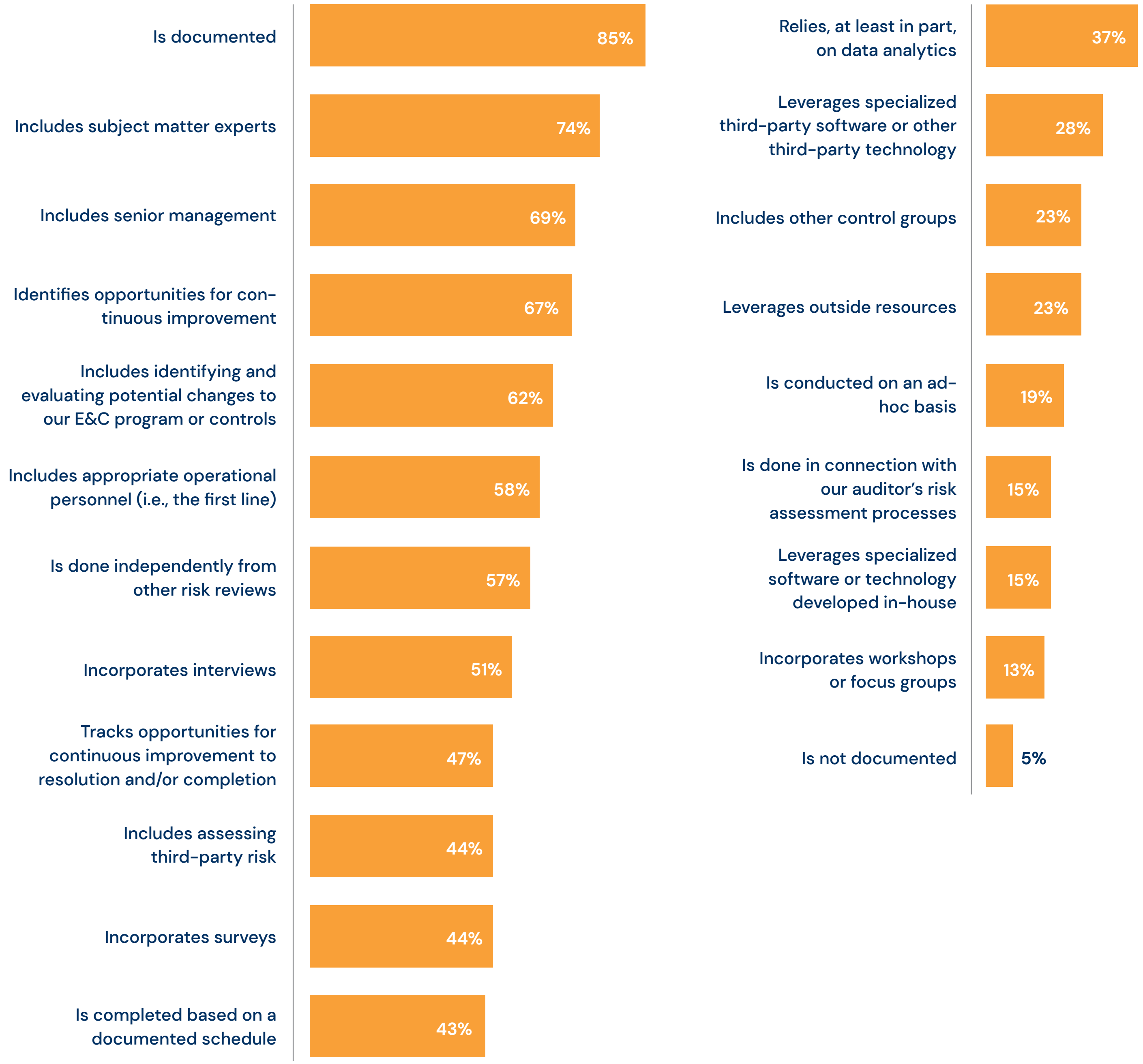
Do you conduct a separate, stand-alone E&C risk assessment at your organization?



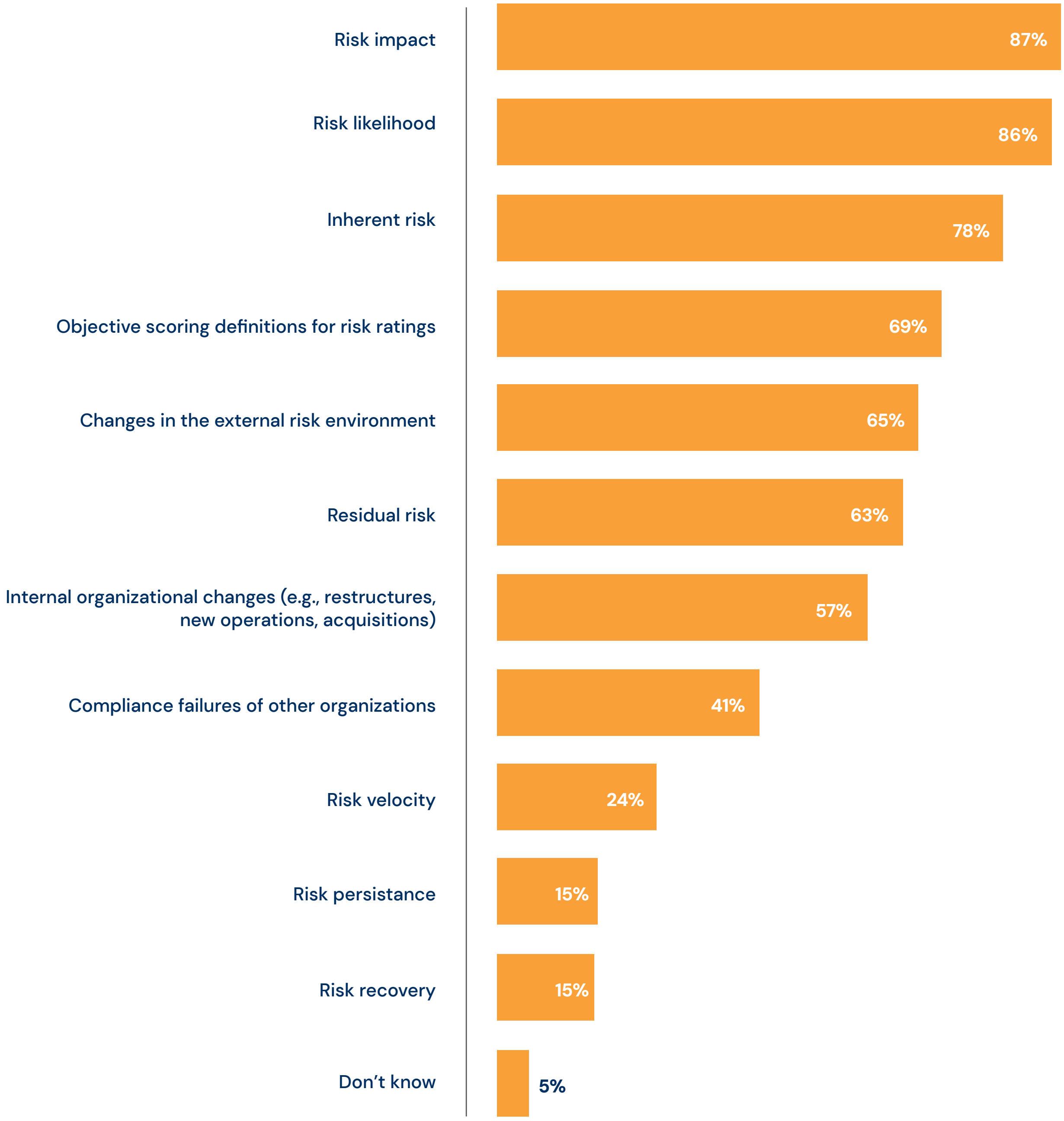
How often do you conduct an E&C Risk Assessment?



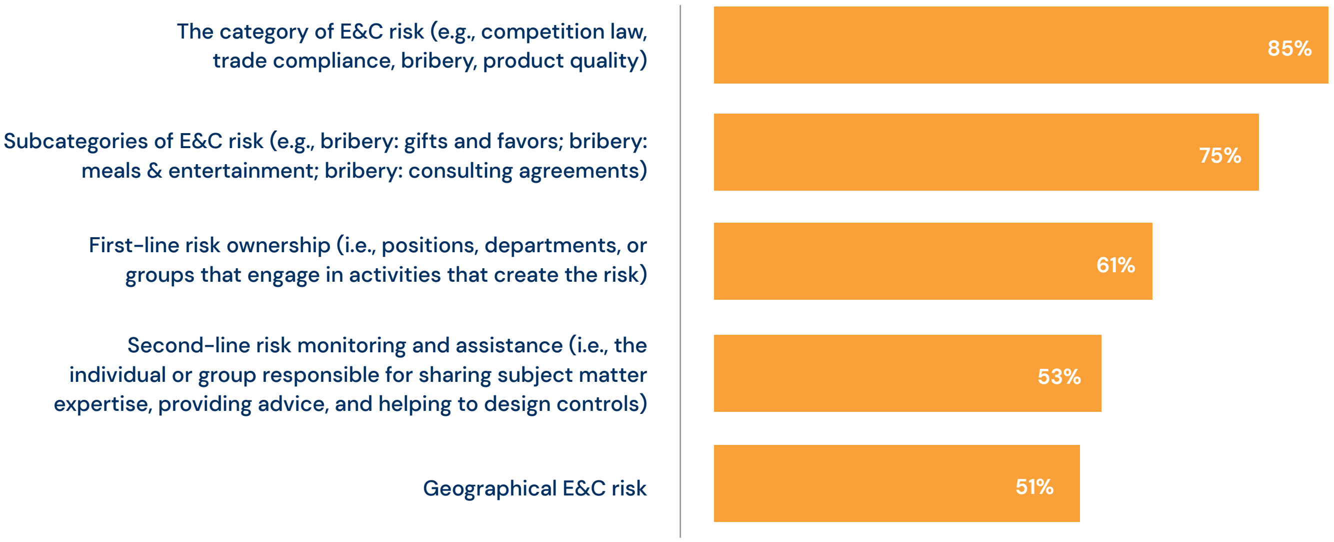
Our E&C Risk Assessment process:



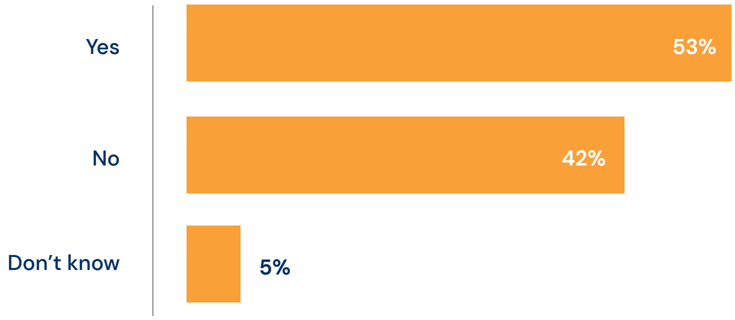
In designing your E&C Risk Assessment, which of the following does your organization consider?



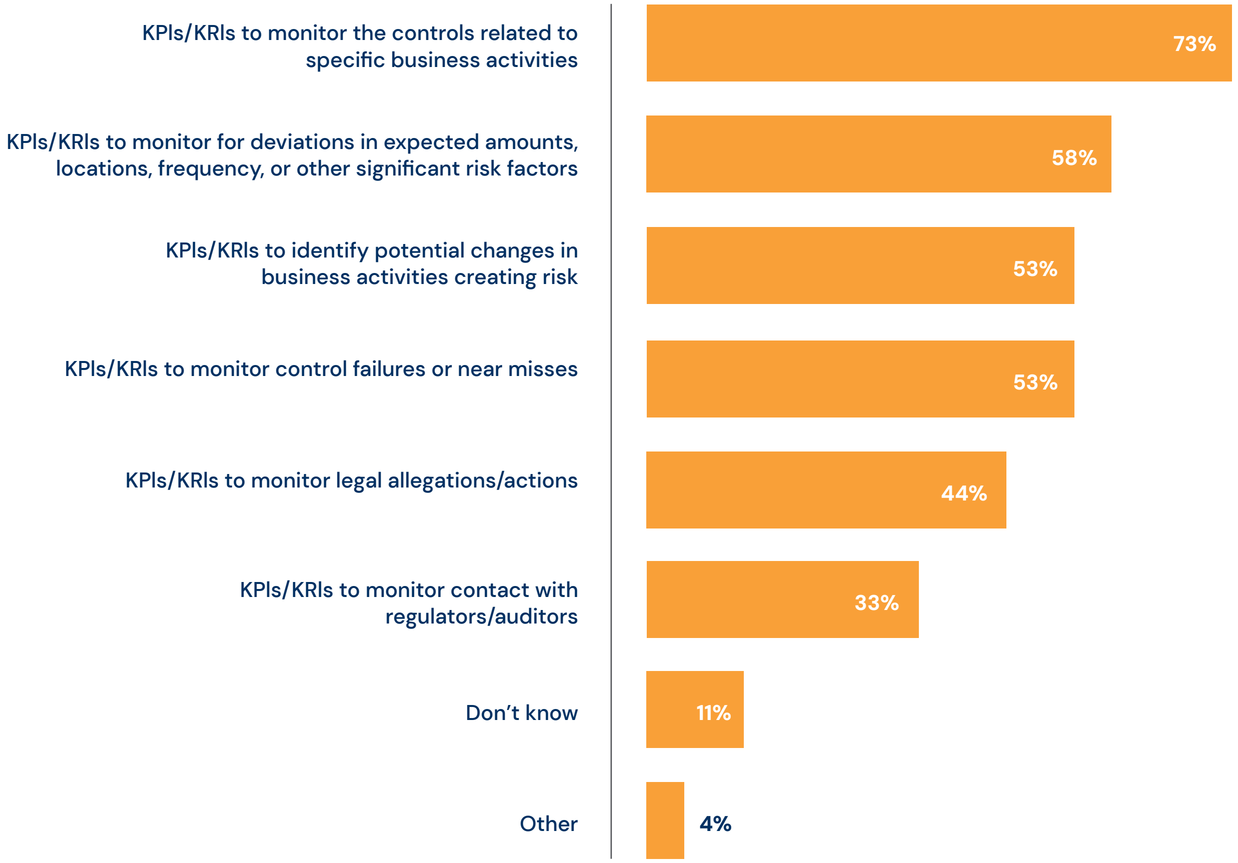
What information is included in your E&C risk universe, E&C risk catalog, or list of risks compiled during your E&C Risk Assessment process?



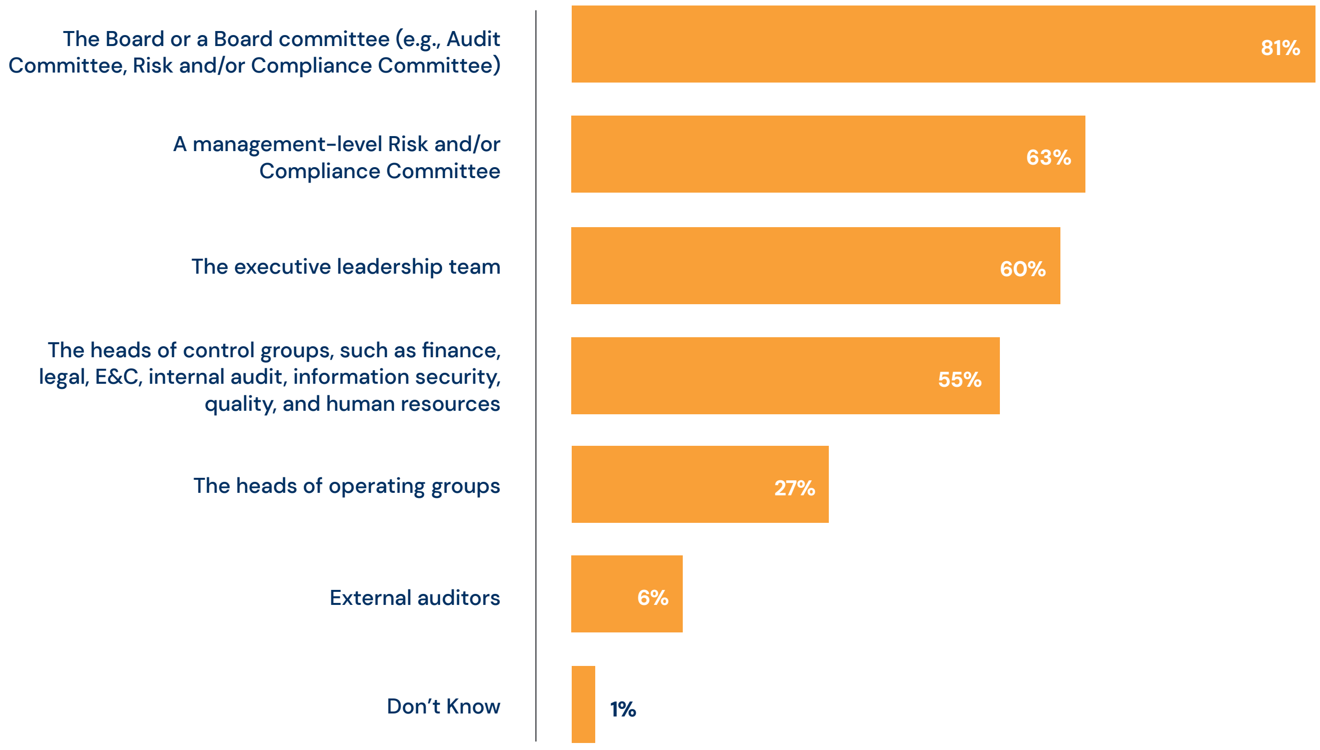
Do you use key performance indicators (KPIs) or key risk indicators (KRIs) in your organization's management of E&C risks?



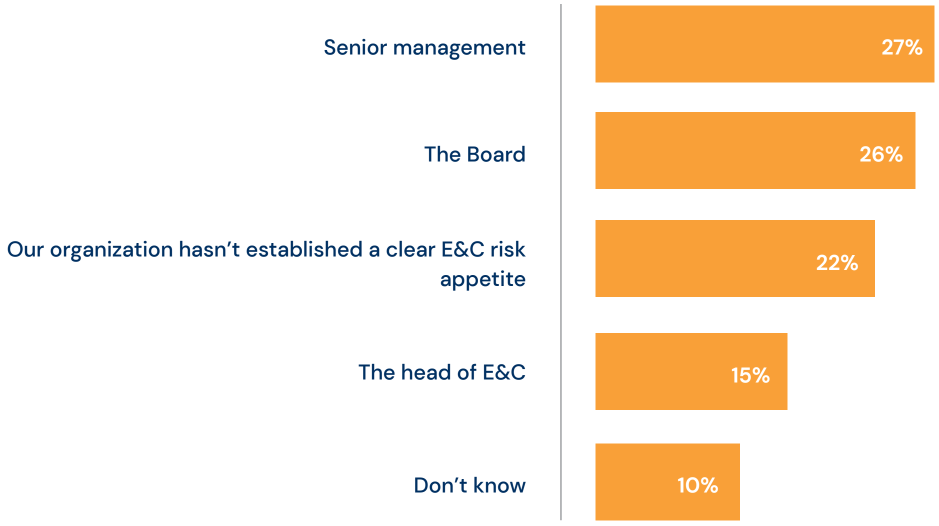
What type of KPIs or KRIs does your organization use in its E&C risk management program?



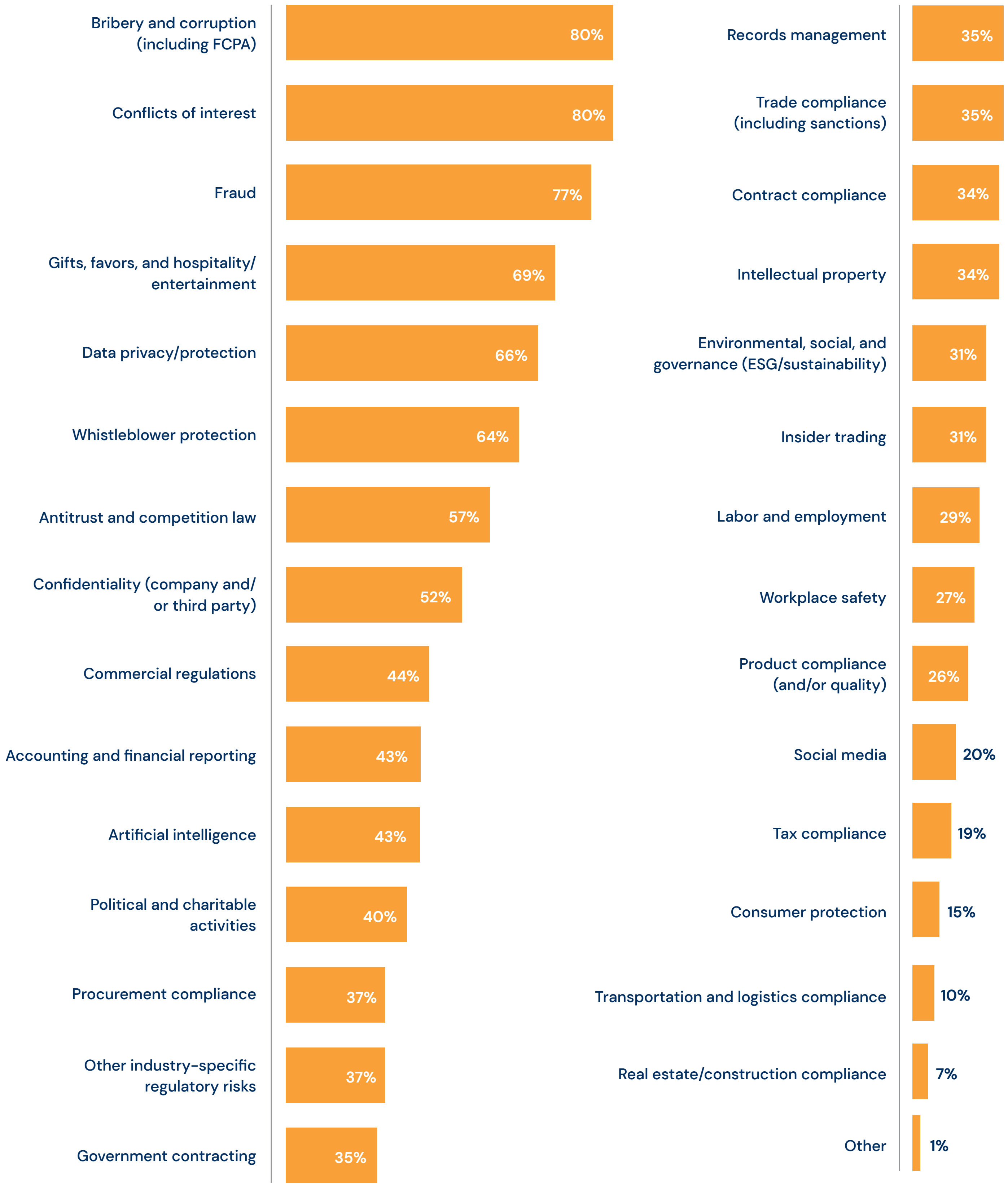
To whom do you report the results of your E&C Risk Assessment?



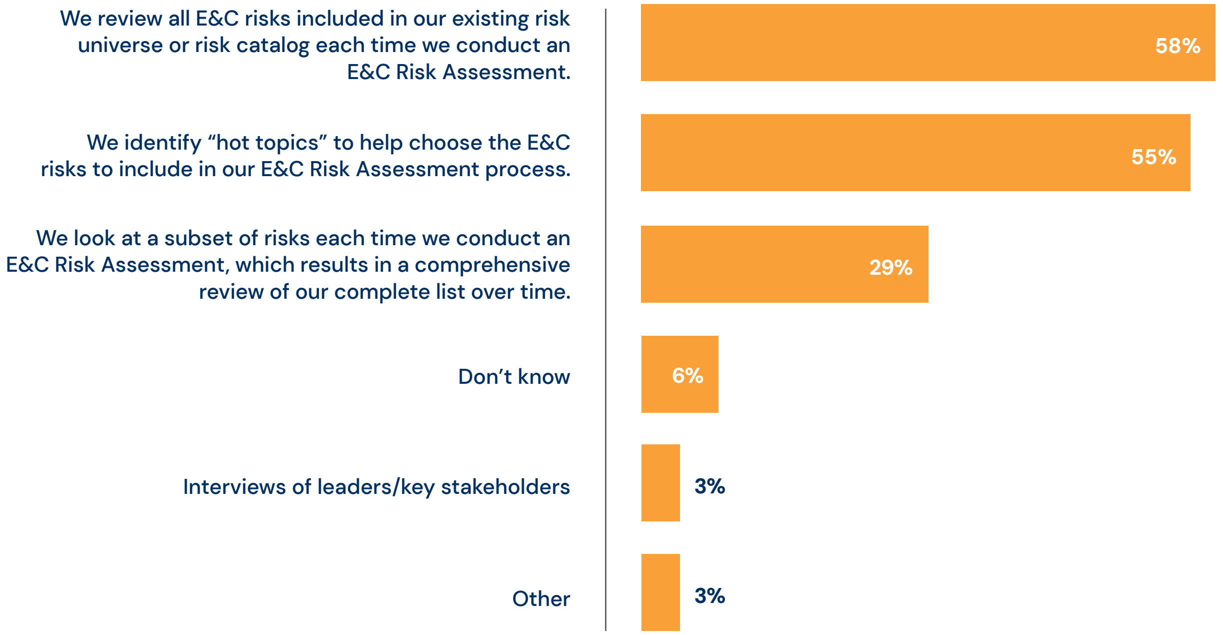
Who sets the E&C risk appetite for your organization?



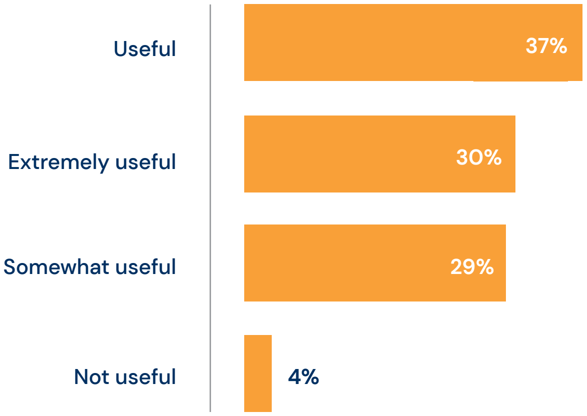
Which of the following risks do you assess in your E&C Risk Assessment?



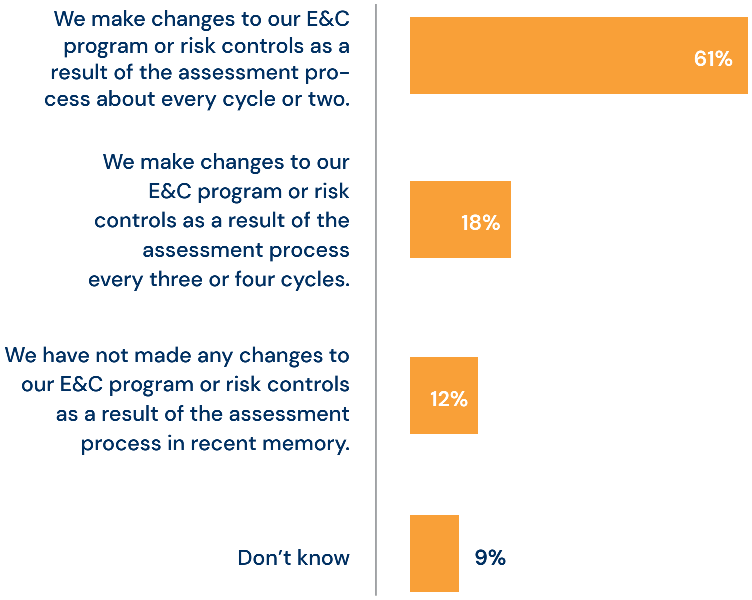
How do you determine which risks to include in your E&C Risk Assessment?



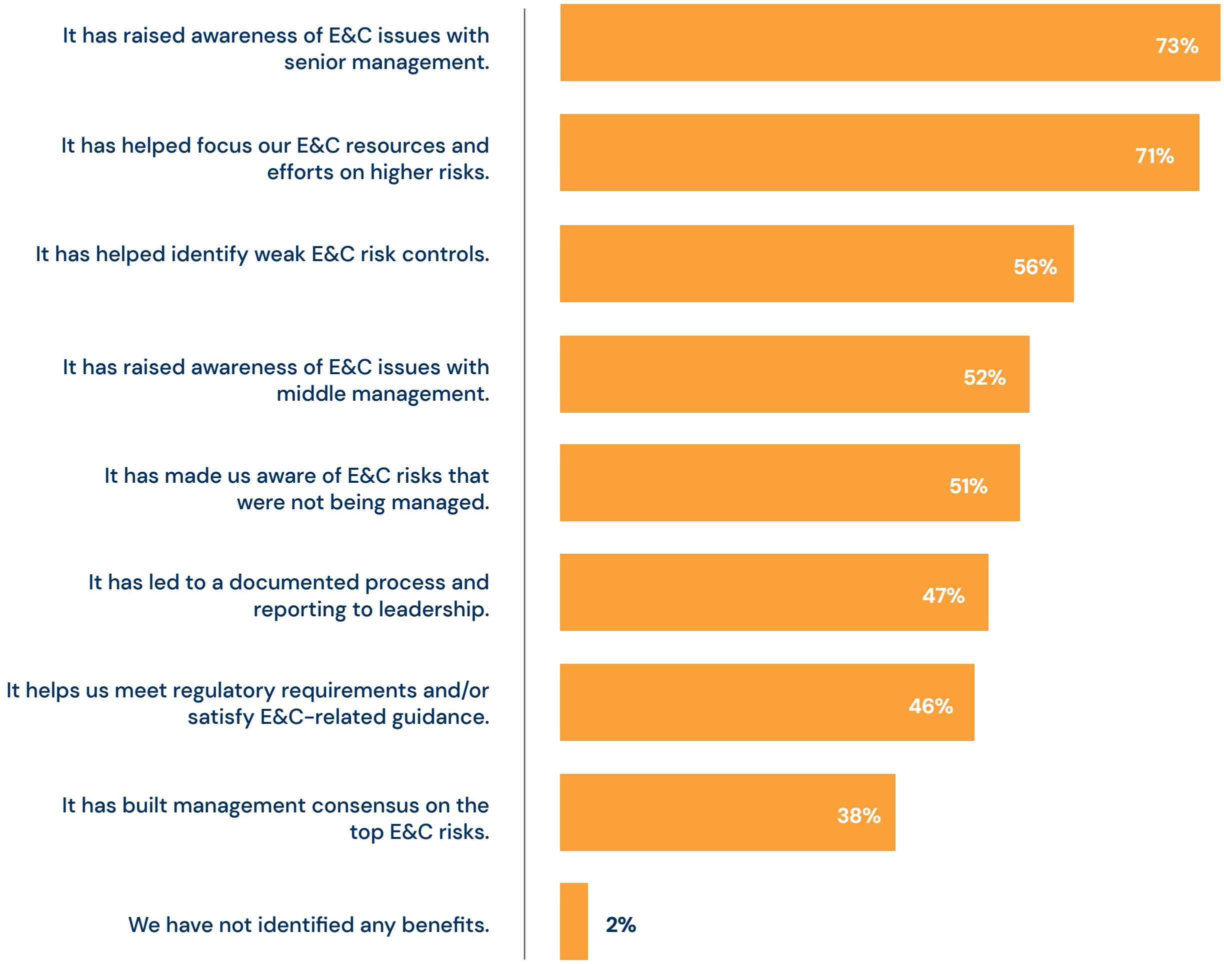
In your opinion, how useful is your E&C Risk Assessment?



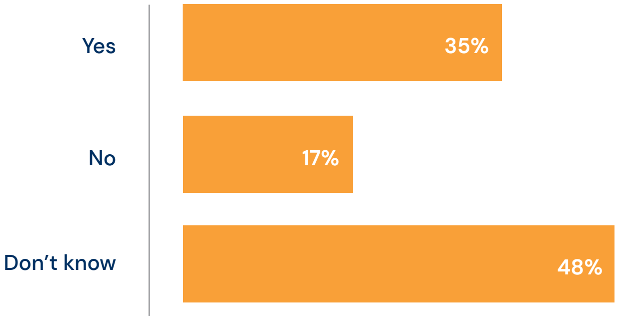
How often does your organization make changes to its E&C program or its risk controls based on your E&C Risk Assessment results?



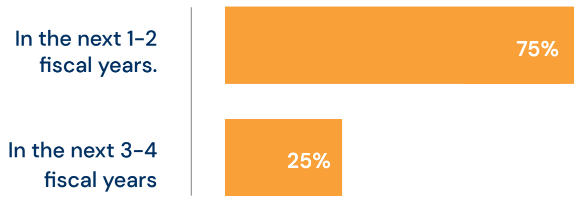
What benefits has your E&C Risk Assessment brought to your E&C risk management efforts?



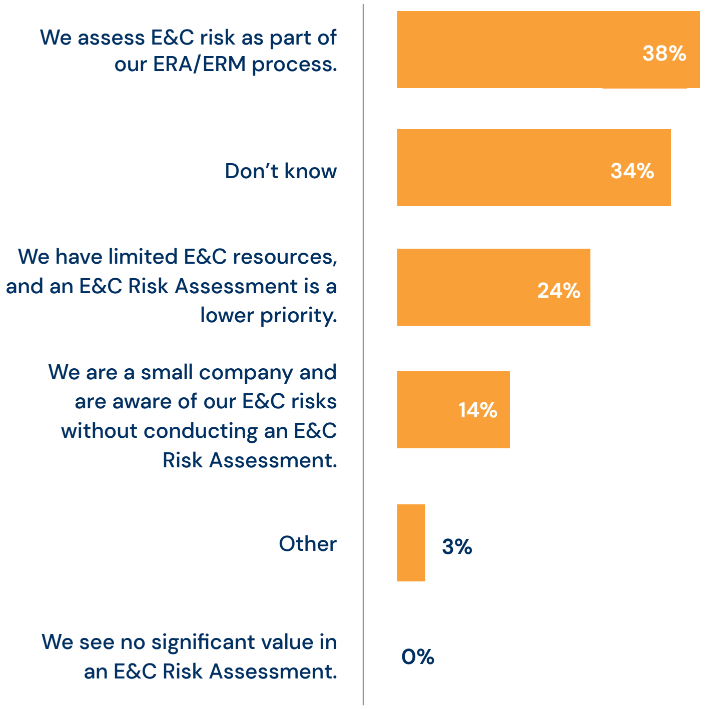
Do you plan to conduct a formal E&C Risk Assessment in the future?



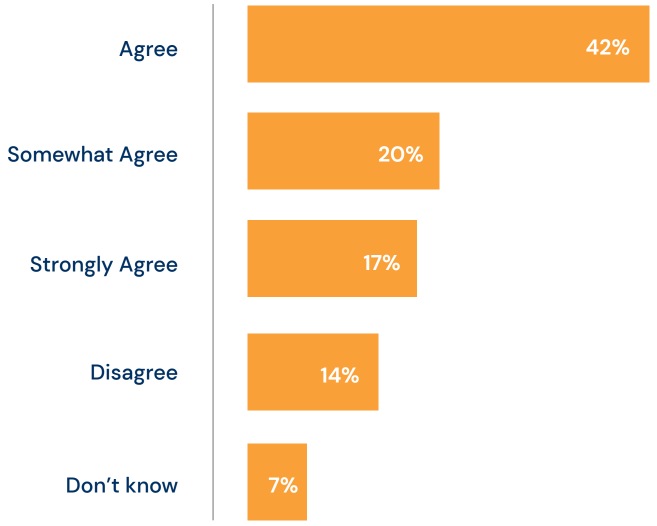
What is your timeline to start an E&C Risk Assessment?



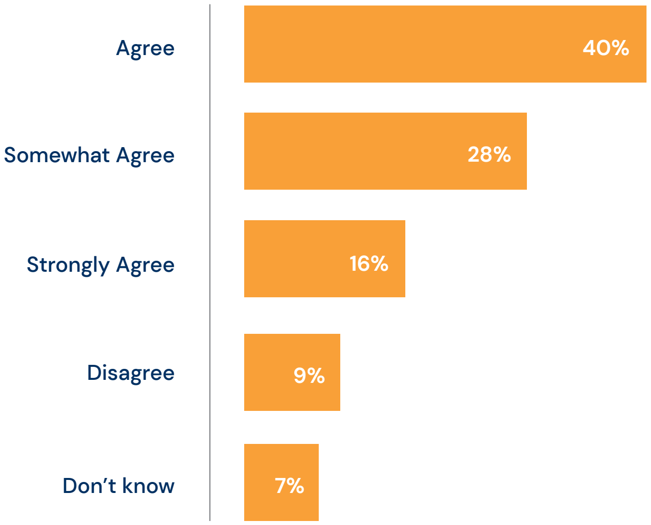
What are the primary reasons for not conducting an E&C Risk Assessment at your organization?



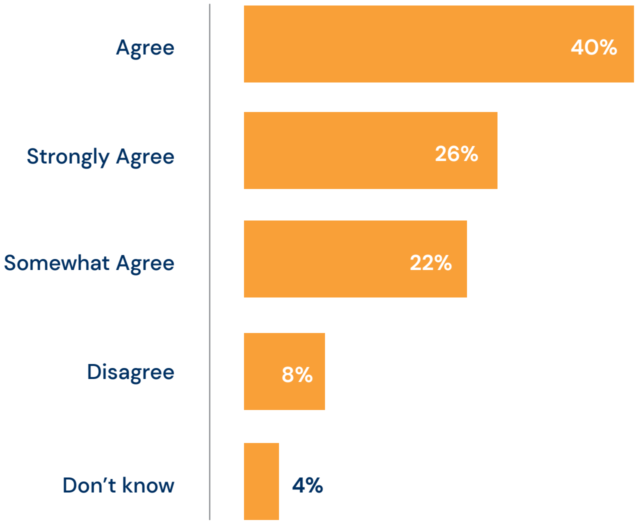
The design of the E&C program at our organization and our available E&C resources are commensurate with the organization's E&C risks.



At our organization, there is a strong correlation between the highest E&C risks and the controls and resources dedicated to managing those risks.



Our E&C training program is informed by our E&C Risk Assessment results.


Agree
Strongly Agree
Somewhat Agree
Disagree
Don’t know